Project AIR FORCE

WHO RUNS WHAT IN THE GLOBAL INFORMATION GRID

WAYS TO SHARE LOCAL AND GLOBAL RESPONSIBILITY

MARTIN LIBICKI

RAND

The research reported here was sponsored by the United States Air Force under Contract F49642-96-C-0001. Further information may be obtained from the Strategic Planning Division, Directorate of Plans, Hq USAF.

Library of Congress Cataloging-in-Publication Data

Libicki, Martin C.
Who runs what in the global information grid? : ways to share local and global responsibility / Martin Libicki.
p. cm.
"MR-1247-AF."
ISBN 0-8330-2888-X
1. Communications, Military—United States. 2. Command and control systems—United States. 3. Military intelligence—United States. 4. Aerial reconnaissance—United States. 5. Space surveillance—United States. I. Title.

UA943 .L53 2000
355.3'432'0973—dc21

00-062730

Published 2000 by RAND
1700 Main Street, P.O. Box 2138, Santa Monica, CA 90407-2138
1200 South Hayes Street, Arlington, VA 22202-5050
RAND URL: http://www.rand.org/
To order RAND documents or to obtain additional information, contact Distribution Services: Telephone: (310) 451-7002; Fax: (310) 451-6915; Internet: order@rand.org

Project AIR FORCE

WHO RUNS WHAT IN THE GLOBAL INFORMATION GRID

WAYS TO SHARE LOCAL AND GLOBAL RESPONSIBILITY

MR-1247-AF

MARTIN LIBICKI

RAND

Prepared for the United States Air Force

Approved for public release; distribution unlimited

PREFACE

This study was prompted by a question circulating through the U.S. Air Force: Should it step up to assume the responsibility for providing all operational information to warfighters throughout the Department of Defense (DoD) (and possibly beyond)? DoD is already beginning to consolidate information systems that support command, control, communications, computers, intelligence, surveillance, and reconnaissance (C^4ISR); logistics; etc. Among the military Services, the Air Force believes itself to be the most deeply embedded in the information business (notably, but not exclusively, through its space activities). So it seems like a natural commitment to make.

But is it? Even if one grants the inevitability of widespread networking and thus global access to all sorts of information (as well as the desirability of greater jointness), does it therefore follow that *some* entity—be it the Air Force or some other organization—must take charge of developing, integrating, populating, and thus operating DoD's entire C^4ISR apparatus?

The global provision and management of information has its virtues. It exploits global sensors and provides an initial basis for interoperability, economies of scale, and a coherent rationalization for spending information dollars. But if connectivity is ubiquitous, local provision and management of information leads to a system that is more sensitive to user requirements and more adaptable to local contingencies. Because some information is clearly global (e.g., detecting launches of intercontinental ballistic missiles) and some clearly local (e.g., a warfighter's after-action report), the issue is not either-or, but the right balance along the global-local continuum.

This report focuses on information collection and information services. It concludes by recommending a bias toward a standard architecture and toward decentralized management—an Internet-like approach.

The study was conducted as a direct assistance project for the Air Force under the sponsorship of the Deputy Chief of Staff for Plans and Programs and the Assistant Deputy Chief of Staff for Strategic Planning. It should be of broad interest to the Air Force community, to the C^{4}ISR community in general, and to those beginning to think about the command and control of information in particular.

PROJECT AIR FORCE

Project AIR FORCE, a division of RAND, is the Air Force federally funded research and development center (FFRDC) for studies and analyses. It provides the Air Force with independent analyses of policy alternatives affecting the development, employment, combat readiness, and support of current and future aerospace forces. Research is performed in four programs: Aerospace Force Development; Manpower, Personnel, and Training; Resource Management; and Strategy and Doctrine.

CONTENTS

TABLES

SUMMARY

Traditionally, information was used to provide commanders with broad situational awareness, leaving operators to rely on what their own senses provided (quintessential local data) in order to conduct combat. In the last 50 years, the advent of sensors and their ever-lengthening range, coupled with the ability to digitize information and distribute it globally, have changed all this. The campaign in Kosovo was largely fought using global information: Sensor-acquired data on Yugoslavian targets were often analyzed far from the front and converted into aim points for precision-guided weaponry.

The rise of global information in turn suggests that DoD's information systems as a whole should be agglomerated into what has been variously referred to as a "System of Systems" (from Admiral Owens); "Battlespace Infosphere" (from the Air Force Science Advisory Board); or, the term now favored within the Office of the Secretary of Defense, the "Global Information Grid (GIG)" (or, in the shorthand used here, the Grid). The GIG was formally defined in the memo from the Assistant Secretary of Defense, Command, Control, Communications, and Intelligence dated September 22, 1999, as

> The globally interconnected, end-to-end set of information capabilities, associated processes and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel.

In any event, as part of the GIG effort, the DoD's integration of its various C4ISR assets is proceeding.

The question has thus arisen in the Air Force whether some institution should volunteer (and be resourced) to program, acquire, integrate, manage, and operate such a system. Should the Air Force—which believes itself to be more deeply embedded in the information business than are its sister Services—take charge of providing operational information to all warfighters? Without delving into the question of whether the Air Force, another entity, or a new creation is the right organization to take charge, the real question should be: Should *any* entity assume that role? The question quickly turned out to be nuanced. Clearly, there are information sources and services that have to be globally provided (e.g., scanning for ballistic missile launches from space). Equally clearly, there are information sources that must be locally provided if they are to exist at all (e.g., a warfighter's after-action report). So, the question is less one of whether there should be global information systems (there are, and there will be) than one of where the best place is to draw the line between global and local responsibilities for providing information and information services.

ASSUMPTIONS

In answering such a question, several assumptions need to be made:

- The subject is limited to C4ISR and combat support.
- The acquisition of client equipment (e.g., computers, network concentrators) is assumed to be a separate question (addressed in Appendix A).
- Background intelligence (e.g., prevailing characteristics of other nations' assets, strategies, plans) is assumed to be a global responsibility.
- Local may be typified as a commander of a ship, battalion, or squadron. Information assets actually report to many echelons, so in some cases, a regional stratum controlled at the commander in chief (CINC) or joint task force (JTF) level may have to be considered part of the mix.

- The focus is on who operates rather than acquires the information systems that make up the Grid.
- The choice of who is responsible for an information system need not dictate who can see its information or at what stage in processing information becomes available.
- The reference conflict includes local operations and takes place circa 2008.

CANONICAL ARGUMENTS FOR AND AGAINST CENTRALIZATION

Difficult problems of coordination coupled with potentially overlapping responsibilities in any complex endeavor often raise demands that someone be placed in charge of an enterprise. Power is concentrated on those with the onus of making something work. One line of justification for globalizing a large chunk of the Grid can be expressed in terms of cross-Service rationalization, an improved ability to program resources for information coherently, and a presumption of interoperability (central operation, in turn, maintains these advantages in the face of user-generated entropy). The other justification is that centralized operation promotes consistent and optimized sensor coverage of the battlespace, permits various elements of the Grid to be tightly integrated, and makes it easier to mobilize information flows to support allies (especially when U.S. forces are not directly involved in fighting).

The disadvantage of centralization is that coherence in the information dimension often comes at the expense of coherence between information and operations. Local control of information systems (1) helps information better fit its warfighting uses, (2) encourages and forces warfighters to understand their urgent information needs and allocate scarce resources against them, and (3) facilitates user adaptation and innovation. But while such arguments echo those that favor markets, the military has an entirely different command-and-control culture, a difference not to be ignored lightly.

WHO SHOULD SUPPLY THE DATA?

Sensors play a key role in determining who gets what information: They are the source of raw data. They are also expensive, scarce, and subject to command and control. This fact brings up two competing models for determining which functions are best global and which are best local. One is to build information systems around sensors (whose technical characteristics then suggest what echelon would manage them) and to provide their data in processed form to the Grid. The other is to build (virtual) information systems around the support of specific missions and to use sensor requirements to make a first-cut determination of where such systems as a whole should be managed.

The sensor-centric approach replicates today's architecture but, in doing so, focuses more on the tools than on the task. Putting sensors under different fiefdoms vitiates the integration across sensors that may become increasingly valuable and complicates the task of warfighters, who should benefit from being able to call on each at will. As technologies change or other circumstances (e.g., where U.S. forces are based) change, how situational awareness is acquired will—or ought to—change as a result. Bureaucracies formed to manage specific tools will resist the decisions of others to carry out tasks with alternative ones that challenge their status.

The mission-centric approach asks what data are needed to support a mission and, next, who is in the best place to organize them. It also suggests advantages from providing operational information as a set of overlays: Fundamental data come from mapping, intelligence, and global sensors, atop which regional and then local data are successively overlaid. The approach runs up against the problem of sensor contention and thus suggests the value of developing tools for easily moving command over specific sensors up or down the hierarchy, as need dictates.

WHO SHOULD SUPPLY THE SERVICES?

The more pervasive networks become within DoD, the richer the set of systemic—and hence, globally provided—services that can be provided for warfighters. But not all or even most globally provided services need come from the same entity.

Economies of scale in analysis, for instance, argue for their concentration. But the ability to move bits anywhere suggests that, in rare cases (when the needs of analysis strongly affect what data are collected and how), analysis need not be done by the same entity that collects the data. Indeed, analysis may be a value-added activity for which users make specific arrangements.

Other systemic services include (1) the development and maintenance of tools that help operational units coordinate actions with their counterparts, (2) applications to inform users about the existence and quality of new information on the Grid, (3) network management, and (4) the distribution and maintenance of access and/or usage privileges with an emphasis on security. Standards and cross-service access are also inherently global functions.

If the Grid is to have a core (that is, a set of services managed by the same entity), it would likely include global network management; the distribution of privileges; and advocacy for standards, cross-Service access, and resource rationalization—but not tools, systemic applications, and regional network management.

CONCLUSIONS AND RECOMMENDATIONS

The result of all this cogitation is to cast favorable light on many operational maxims that have made the Internet a success. But due account must be taken of the Internet's weaknesses (too little security, too much junk, and low support for urgent applications) and the fact that market mechanisms for satisfying business needs are weak or absent within DoD. Four recommendations follow:

- DoD should exercise a strong bias toward interoperability as a way to foster universal access to information. Achieving this, in turn, calls for an entity (e.g., a honed-down Defense Information Systems Agency, an Air Force–led joint office) that can architect the Grid to that end.
- The achievement of interoperability, in turn, should permit a strong bias toward local provision of operational information and vigorous sharing, both horizontally and vertically, to build a battlespace picture. To this end, liberal distribution of unit-level sensors and connectivity should be encouraged.

- Overlay technology should be advanced so that local and global information sources can fit together more easily.
- Some entity within DoD should review the extant suite of systemic services and lay out a road map for filling in the blanks.

All this gets us back to the initial question: Should the Air Force provide information superiority for all warfighters regardless of Service? Our conclusion is no—not the Air Force and not any other entity. What is needed are the tools that permit the users in the field (variously defined as the CINCs on down) to create whatever information tableaux best fit their needs at the time.

ACKNOWLEDGMENTS

Special thanks go to Dr. Clark Murdock (now a professor at the National Defense University) for his sponsorship, advice, and support. There is nothing so valuable in analysis as to start off with a good question, and Dr. Murdock's restless mind has, over years of interaction, provided more than his fair share. Thanks are also due to the many colleagues and friends who have read and made extensive comments on this report, notably RAND's David Signori, but also Major James Marrs (USAF), Robert Anderson (RAND), Ray Evans (MITRE), Jeremy Shapiro (RAND), Louis Marquet (CECOM), Arthur Ballato (CECOM), and Phyllis Gilmore (RAND).

ABBREVIATIONS

BDA	Battle damage assessment
BMEWS	Ballistic Missile Early Warning System
C^4ISR	Command, control, communications, computers, intelligence, surveillance, and reconnaissance
CEC	Cooperative Engagement Capability
CINC	Commander in chief
COP	Common operational picture
DISA	Defense Information Systems Agency
DLA	Defense Logistics Agency
ELINT	Electronic intelligence
GCCS	Global Command and Control System
GIG	Global Information Grid (also, the Grid)
GPS	Global Positioning System
JTF	Joint task force
MTI	Moving-target indicator
NATO	North Atlantic Treaty Organization
NRO	National Reconnaissance Office
SAR	Synthetic aperture radar
SBIRS	Space-Based Infrared Radar System

SEAD	Suppression of enemy air defenses
SOSUS	Sound Surveillance System
TMD	Theater missile defense
UAV	Unmanned aerial vehicle

Chapter One

INTRODUCTION

Once upon a time, information was collected primarily to inform command rather than operations. A well-prepared army (or navy) poised for battle would be armed with intelligence on the enemy's strategies, operational objectives, doctrine, weapons, and morale—all global in nature and external in source—as well as the location of its forces. So apprised, an army (or navy) would try to engage the enemy at a time, place, and manner of its own choosing. Yet once battle was joined, operational information on the enemy was local and even personal. Soldiers shot or thrust at what they saw ahead, relying on their eyes for information, ears for coordination, heads for analysis, arms for attack, and mouths to report on their fight.

Even as late as 1991, U.S. forces in the Gulf War's Battle of 73 Easting, while well-briefed on what they expected to find, nevertheless sighted enemy armor themselves, calculated the range and bearing of enemy tanks, fired their weaponry, and recorded the results in memory (and, only later, digitally). The substitution of mechanical for biological systems did not detract from the fact that almost all of their *operational* information was local.

Fast-forward eight years to Kosovo and replace the tank with a B-2 bomber carrying cruise missiles. Data on the target are captured with long-range sensors (e.g., satellites, or maybe unmanned aerial vehicles [UAVs]), analyzed using complex computer models (e.g., of Yugoslavia's transportation system), and converted into aim points. The target is matched against its weapon (a cruise missile), which is loaded on the aircraft. The aircraft flies forward, its pilot briefed on the likely threat (a nominal one if the aircraft never crossed into

Yugoslavia). Target updates are fed to the bomber (and its missile) in midflight. At some point, the bomber releases its missile, which hits the target. Battle damage assessment (BDA) is provided by sensors similar to those that identified the target in the first place. Both intelligence and operational information are *globally* provided. Were cruise missiles launched from submarines, there would have been even less threat to worry about, and thus even less local information would be needed. Ten years hence, a similar scenario could be written about a tank engagement against over-the-edge targets spotted by external sensors.

Trends are clearly driving the U.S. military toward using more global than local information. The basic reasons are familiar. Long-range sensors see farther and faster than humans can. The Global Positioning System (GPS) permits information to be embedded with latitude and longitude data for accurate geospatial plotting. Long-range weapons permit distant but precisely mapped targets to be struck. Ever-growing aversion to casualties feeds the U.S. preference for action at a distance. New information technologies mean that global information can be requested, gathered, analyzed, and used in an engagement as it is taking place. An essential premise of new warfare theories would have tomorrow's warfighter enter combat armed not only with general intelligence on the enemy but with operational information that illuminates the enemy's precise whereabouts. This picture would look the same in Colorado Springs as in Kosovo: global knowledge, globally accessible. Planning for this agglomeration—the Global Information Grid (GIG, or, as used here, the Grid)—is under way, pursuant to the memo from the Assistant Secretary of Defense, Command, Control, Communications, and Intelligence dated September 22, 1999, which defines the GIG as

> The globally interconnected, end-to-end set of information capabilities, associated processes and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel.

Nevertheless, even if information superiority from a Grid fed by and feeding all is the *eventual* prerequisite to military superiority (as *Joint Vision 2010* preaches), does it therefore follow that some central institution should be responsible for ensuring the quality, availabil-

ity, and timeliness of its products and services (a question similar to but distinct from whether the Department of Defense [DoD] should form corps specialized to manage information)? Or should several such institutions exist? How deeply should its (or their) authority run? Should global institutions provide a baseboard of information, or should their responsibilities be extended to *all* operational information—or somewhere in between? And if so, what criteria should be used to divide the tasks? Global providers should not have to provide what is better supplied locally, and users should not have to acquire what is more efficiently supplied globally.

These questions grow out of a concern that has surfaced within the U.S. Air Force. As a broad consensus has formed in favor of some overarching information system to guide warfighting, it has been suggested that the Air Force take charge of developing and running it. For historic reasons, including its heavy involvement in space, the Air Force's share of the information business exceeds that of its sister Services (some defense agencies are more highly concentrated in information, but they are smaller and not responsible for warfighting). Yet, the bill for taking *all* this responsibility may be stiff. Information accounts for at least $50 billion of the DoD budget (the standard sum of all information activities) or more (adding all weapons, sensors, logistics databases, system administration, etc.). Air Force budgets will have a hard time expanding to accommodate all that. Having the Air Force run everything is also untenable: Imagine it flying E-2s off aircraft carrier decks, much less operating Aegis cruisers or manning Sound Surveillance System (SOSUS) arrays. It is harder to imagine passing this mission to an organization not composed of warfighters.

The more fundamental issue is not whether the Air Force should or should not be the predominant Service agent for operational information (answering that would require assessing the culture, doctrine, and competence of the Air Force against those of other contenders). The going-in question is whether *any* entity should be made responsible for engineering the Grid, acquiring its global elements (Appendix A speaks to who buys local elements), and operating it (including exercising command and control over such fielded elements as sensors and long-haul communication devices). Yet further refinement is in order because global command and local control are ideal types. DoD missions vary greatly; so do the information

services that ought to be in the Grid. Some are better off being provided primarily by a single global source; others are better if developed by or at least for their ultimate users; still others require a mix of global and local contributions. What criteria should be used to determine where along the global-local continuum the responsibility for providing such services should lie? Inherent in this question are others. What are the principal mission areas that go into information superiority? Should there be a single authority for determining what and how much goes into it? To the extent the Grid has a single unified interoperable network architecture, how much should its design, acquisition, integration, and operation be centralized? What issues and design features cut across mission areas and technical domains so much that cross-cutting integration is also required?

This report thus has two foci. The primary one is what information ought to be provided globally (that is, by entities sitting outside the operational chain of command) rather than locally (that is, directly by warfighters)? The secondary one is the role of the *core*—the portion of the Grid's contents, infrastructure, and protocols that is under the control of a single designated entity within DoD. The question of *who* might run the Grid—the Air Force versus someone else—is a question for another day.

WHAT IS AT ISSUE?

One way of grasping the nature of the global-local continuum is by examining two opposite scenarios for organizing the generation and distribution of military information and information services.

In the global scenario, DoD is organized around the provision of information as a central function. A joint entity (or a defense agency) is charged with ensuring that warfighters receive situational awareness: complete background intelligence; access to global databases (e.g., logistics, medical support); and, notably, various recognized pictures in requisite detail. The recognized air picture, for instance, is built by fusing data from a variety of sensors from space and air (both manned and unmanned) to ground (such as air defense radars). There are counterpart pictures for other media: sea, ground, electromagnetic, cyberspace, etc. Analysis of these pictures for gaps and hot spots determines where resources for coverage and analysis

are to be concentrated. Resources to emplace and operate sensors are put under direct control of the Grid's managers, either at the national or at the theater level, who also organize the gathering and analysis of field reportage, ensure capacity between the Grid and the users, and provide services to enhance the information's usefulness. Warfighters have input into the process as warfighting commanders and customers; their wants and complaints are duly noted.

In the local scenario, warfighters build their own information picture. National sensors (notably, satellites), some long-haul communication infrastructures (the rest are leased by commanders in chief [CINCs]), and background intelligence are globally provided—but little else. Local users determine their information requirements; deploy the sensors needed to get the information (or acquire effective control over higher-level sensors when in their area of responsibility); arrange for the analysis (e.g., data fusion), cross-cutting data, or applications needed to make sense of the readings; and use this information to fight the war. If warfighters need information from their counterparts across the way or in other media, they negotiate for adequate coverage or leave it to higher-level commanders to order as much. Commanders keep certain information resources in reserve so that they may be committed to sway the outcome of battle.

In some ways, the global-local distinction echoes information push-versus-pull debates (even if global-local is more about making information and push-pull about taking it). A global orientation suggests information push at least in the sense that the meal is prepared by others for the presumed taste of the customers. A local approach is more clearly information pull; nothing is made until it is ordered. But does information always flow down to users? Local information can also inform global decisions. Target lists in Kosovo were based, in part, on often-local BDA. The Desert Storm cease-fire was based on (alas, incomplete) local information that reported Iraqi forces to be surrounded by Coalition forces. Local units feed the global information apparatus, collecting information not for themselves (other than to keep out of trouble) but to inform those up the chain.

A better corollary issue may be whether information ought to precede or follow operations. That is, should information be gathered before there is (and in many cases, to suggest the need for) a requirement to support specific military operations, or should mili-

tary operations alone suggest what information needs to be collected? A global information provider works around the clock in good and bad times (as intelligence agencies do today). It scans the globe, looks for dangerous anomalies, and uses the results to inform policy and, if necessary, the direction of forces. To the global provider, coverage, continuity, and history are important. Coverage matters because areas left unseen are sources of surprise; if foes know they are unseen, bad surprises are more likely. Correlation builds knowledge by suggesting whether otherwise unrelated events reflect a deeper source or by permitting more generalized comparisons and contrasts. History matters because it permits change detection and greater insight about the context of anomalies. All three drive global providers to gather similar data across space and time.

A local information consumer, by contrast, starts with the immediate task at hand and examines the prerequisites to its accomplishment. One of these prerequisites is to increase knowledge, and the search for such knowledge induces the distribution of sensors, the gathering of reports, and the establishment of analytic capability. Whatever information is gathered is uniquely specific to the task and is largely irrespective of global consistency. When the task is done, information resources are reallocated. For obvious reasons, global managers look first to global sensors to do a job, but local users would look toward local sensors to do the same thing.

In practice, some global-local issues are really ones of multiple choice. In a modern military, command can pivot in many places. Within just the Department of the Navy, a carrier battle group fights as one integrated unit (under a rear admiral); submarines and deployed air strike packages operate as smaller units (under a naval commander); and marines and special forces operate as squadrons (under lieutenants and captains). Assets considered local to big units are global to small units. Whether information from, say, a high-altitude UAV is local or global depends on the perspective. To the joint task force (JTF) commander, it is local; to the battalion commander, it is global. A third category, regional, could be used to describe CINC/JTF assets. At the regional level, commands are joint, and their supporting information systems (e.g., the recognized air picture) are often jointly acquired. Regional is local in that it represents the warfighter and is global by virtue of size. Everything higher (i.e.,

national-level systems) are unambiguously global. By contrast, local may be typified as the *commander of a battalion, a ship, or an air squadron*, the lowest level that enjoys a complete information suite in combat (e.g., a ship's combat information center or a battalion tactical operational center).

KEY ASSUMPTIONS

Understanding the right breakdown between global and local information responsibilities requires making assumptions about what constitutes information systems, what differentiates global providers from local users, and what kind of war is at issue.

First, the information systems in question are limited to those that support operations: notably, command, control, communications, computers, intelligence, surveillance, and reconnaissance (C^4ISR), but also logistics and medical information. Specifically outside the analysis (although potentially a part of the GIG) are financial information systems, personnel administration systems, and generic office automation.

Second, the acquisition of local equipment—such as radios, computers, servers, network wiring, and sensors attached to combat platforms and weapons—will be assumed to be a local responsibility. The arguments over who buys what are orthogonal to those of this discussion but not irrelevant—Appendix A sketches some pros and cons of centralized acquisition.

Third, and by contrast, global providers supply background intelligence: prevailing characteristics of an adversary or an environment, such as its leadership, governance, goals and objectives, strategies, plans, doctrines, infrastructures, information architectures, equipment, and societal characteristics. Almost all such intelligence is globally collected by the intelligence community (supplemented by reports from military assets, such as CINC staffs), often using scarce specially trained people. Analysis often requires mosaic-building techniques that put a premium on global correlation. By contrast, operational information deals with transitory elements: "what's where" data, as well as orders of battle, tactical alliances, recent activities, and actively executed plans.

Fourth, to focus attention on differentiating global from local functions, no distinctions are made among the many providers of global services until the last part of Chapter Four. In reality, almost every defense agency provides some global information, but coordination among each of them is, to be kind, in its early stages. The closest that DoD has to a core provider for global information services is the Defense Information Systems Agency (DISA)—which runs some long-distance telecommunication lines and provides some network services but actually supplies very little information of its own. Various of DISA's programs and initiatives—such as the defense information infrastructure, the common operating environment, the NIPRnet and classified SIPRnet intranets, and the Global Command and Control System (GCCS)—are attempts to provide a top-level coherence to DoD's global information system but are still limited endeavors well short of their intended size and scope. As for the information itself, a good deal of it—geopositioning, meteorology, and various intelligence products—is now provided by the space community. That said, there is no single unified architecture that even covers just space products, although there are nascent architectures that apply to some of them (e.g., the National Reconnaissance Office's [NRO's] Future Imagery Architecture).

Fifth, the discussion focuses on who operates the Grid—that is, collecting the information and providing the services—not who buys or makes programming decisions for the Grid. Granted, the two are correlated. If, say, the Air Force is tasked to provide information for everyone else, it likely will have been asked to build the system that made it possible to provide the information in the first place. Similarly, buyers of information systems are apt to design local information systems as adjuncts to their global systems (the U.S. Space Command, for instance, has a clear preference for imagining computer network attack as something launched from orbiting assets). The conundrum exists because DoD fights Jointly (in theory) but buys (mostly) Service. The CINC/JTF commander and subordinates consume information but, for the most part, pay for neither information nor information services. More confusingly, those who (1) set requirements for, (2) architect, (3) engineer, (4) acquire, and (5)operate a system may each be different from the other. Many of the critical advantages of going global or going local for any one stream of information or information services are determined by

how the information is specified and acquired. A disconnect between global engineering and local operation risks producing a system in which users have too little discretion over how it works. Nevertheless, at the risk—nay certainty—of oversimplification, this essay concentrates on who owns and operates the system at issue and, in the case of services, who provides them.

Sixth, the management of information provision ought not imply similar authority over the information itself (although, in practice, it does). Thanks to automation and digitization (which make it easy to record and transfer data) and networking (permitting data to be everywhere at once), information can have a life of its own irrespective of the technologies on which it temporarily resides. Thus, the command and control of information need not be exercised by the same people and in the same way as it is over information systems. Similarly, the roster of who can receive information need not follow from decisions on who is to generate it. The same holds for analysis: Data collectors need not be the same people as analyzers.

Seventh, the Grid has to support local warfighters. It is easy to imagine conflicts—e.g., strategic nuclear war, and Kosovo (almost)—fought entirely with global information. But to assume that all war will henceforth have such characteristics is to remove all the meaning from this discussion.

Eighth, at the risk of arbitrariness, the reference year for this essay is 2008—neither too soon to be altered nor too late to be totally fictional. By then, DoD should be farther along in building a Grid. It will enjoy computers and networks ten to a hundred times more powerful than today's, UAVs from the Global Hawk to the hand-held tactical birds; the first generation of cheap disposable ground sensors; and perhaps satellite constellations, such as Discover II (assuming it reemerges after hostile congressional action), or the Space-Based Infrared Radar System (SBIRS)-Low (assuming it does not fly afoul of the Anti–Ballistic Missile Treaty).

REPORT ORGANIZATION

The remainder of this report examines trade-offs between the global and local provision of information in several steps. Chapter Two lays out canonical arguments in favor of both global and local provision

(but notes the limited validity of using a market metaphor for the military). Appendix A sketches some pros and cons of centralized acquisition of client equipment. Chapter Three looks at parsing the information requirements of combat by who organizes it, first by reference to where the data come from (e.g., what kind of sensors) and second by reference to the missions being supported. Appendix B runs through 21 different missions to show how the latter criterion works and what other factors may modify it. Chapter Four discusses the provision of information services, such as peer-to-peer coordination, as well as network and other management tasks. It ends by asking what goes into the core. Chapter Five contains conclusions.

Chapter Two

CENTRALIZE OR DECENTRALIZE?

Centralization promotes operational efficiency by concentrating resources and lowering transaction costs; coordination becomes a many-to-one rather than a many-to-many problem. Decentralization promotes allocative efficiency by letting users expend scarce resources on their most pressing problems. It promotes flexibility by permitting all users to adapt their information requirements to their own needs. These are arguments of economists. But are principles of economics—particularly an economics that assumes markets or quasi-markets—applicable? For good and sound reasons, militaries are command-based hierarchies and not markets.

THE CASE FOR CENTRALIZATION

Difficult problems of coordination, coupled with the potentially overlapping responsibilities in any complex endeavor, often raise demands that someone be placed in charge of an enterprise so that power is concentrated in those who then bear the onus of making something work (rather than spread among those who can conveniently point to someone else when it does not). The proliferation of military information systems may merit such a response, for several reasons:

- Global management fills gaps. Having every warfighting unit determine, for itself, what aspects of the battlespace merit scrutiny means certain realms will be covered well and others poorly. Geospatial or temporal gaps complicate the tracking of targets in space and time. Phenomenological gaps frustrate the creation of a full-aspect picture of adversary capabilities. Ene-

mies that understand the distribution of gaps well enough can exploit this knowledge to dwell in the shadows. Even if a JTF commander understands where these gaps are, he or she may lack the power to fix them because of how specialized and stovepiped the equipment is.

- Information coherence may be easier to achieve. Air defense radars are often designed to interoperate so that one cues and another pinpoints. It is possible to imagine a sensor regime in which space-based assets, UAVs, shipborne radars, and unattended ground sensors do the same—but, without a central authority, doing so well and reliably requires considerable coordination.
- Centralized information provision enables new forms of U.S. influence. Although the United States has armed forces second to none, the world is big, and most of it is far away, and taking casualties is increasingly prohibitive. In some cases, it may be more cost-effective (and less politically hazardous) to supply the information without the forces, corralling and making coherent the necessary data flows from among multiple communities. The goal of a single data flow may prove difficult without someone in charge. Uncoordinated information exchange may confuse allies and third parties; it can work only if each local component of the U.S. military exchanges information solely with its foreign component (and if these components can be unambiguously identified). But if they are more joint, funnel their information through a common pipe, or liaise with the same U.S. counterpart, contradictions and variations in the information they get may be counterproductive.

THE CASE FOR DECENTRALIZATION

The disadvantages of designating a global information czardom are that (1) coherence in the dimension of information is often purchased at the expense of coherence in the close link between information and operations, and (2) someone is already in charge of coherent operational and provisioning domains. CINCs are in charge of operating the forces. Services are in charge of training and equipping them. These are primary (and legislatively mandated) missions, while information is a support function—and coherence in

secondary missions should not come at the expense of primary ones. Specifically, local control of information systems (irrespective of who acquires them) can be justified as follows:

- Information requirements must fit their uses. Although the coordination of information across domains has its virtues, the purpose of information is to make decisions (i.e., CINC roles), and decisions are implemented with men and machines suited for the task (i.e., Service roles). Thus information about, say, ship-bound warheads must be expressed as data needed by shipboard weapon systems, such as fleet air defenses, long-range Standard missiles, or close-in weapon systems. Such weapons are, in turn, used as per fleet doctrine. Having the ship commander (broadly defined) determine what information is required to match weapon, training, and doctrine is more coherent than having commanders develop abstract parameters for such information and then having a global provider determine what information meets such parameters (or, worse, meets the parameters the provider deems worthy). If the commander wishes to alter any weapons, doctrine, or parameters, the information requirement has to change. Flexibility and fast response are not encouraged by placing a large, remote, global information provider in what should be a tight loop.
- Local provision gives users what they need rather than what they say they want—and practice permits them to carve their needs to fit their requisition authority. Otherwise, users, unconstrained by having to pay for the information themselves, will ask for the moon. Even if they do not flood themselves with waves of data at the expense of glitters of insight, the cost of collecting, distributing, and securing such information will exceed any budget. As a result, other mechanisms will arise to govern demand. Usually, some central source—either the provider, the budgeteers, or some oversight group—will do so by fiat and *diktat*. Unfortunately, such mechanisms can only guess at what users need. In some cases, their knowledge may come from their own analysis (i.e., prejudice); in other cases, squeaky wheels will get the grease. Users may have input, but without the serious work of constantly making hard choices against limited means, they are unlikely to learn to distinguish very well between what they need and what they want. Because field experience can teach users

that some entirely new information source or service is needed, they are more likely to get such a service if they have the power to develop it themselves—if allowed to do so at all.

- Even if there is global provision, users may fetch information themselves if not satisfied with what they get or how fast or if they are frustrated in attempting to adapt it to their needs. At a minimum, this leads to duplication. Worse, if the global provider has designed a closed system, such local data will integrate poorly with the global data on the system: It cannot be fused, processed, serviced, or easily stored. As it is, many information components are already in the hands of local commanders who are loath to give them up.
- Intrusive global provision creates a potential for confusion in command and control. The Aegis cruiser, for example, has assumed the role of information provider to the fleet. Is that part of the overall information system? Should the ship's information suite be designed by a global provider and given to the Navy—and, if so, would it not be poorly coupled to the craft itself? Should the provider run the Aegis? The same question could be multiplied through each Service—information is so central to warfighting that an overly expansive global provider could end up running the interesting part of everything.
- In austere, hazardous, or heavily jammed environments, depending on external information sources and services carries great risks. At the very least, commanders need backup capabilities, e.g., field-level UAVs, as well as high-altitude UAVs or satellites, and maps on CD-ROMs (or even paper) rather than on line. Having backup capabilities suggests that the ability to replicate global information sources and services. This Means that hazard does not mandate local provision. And some new technologies can cut through enemy-induced clutter (e.g., phased array antennas can increase the confidence with which fielded units can access satellites by pointing at them).

SOME LIMITS OF ECONOMIC LOGIC

Local provision is supported by arguments that echo those offered for competitive markets. Regardless of how well global providers understand the operators, empowering them to get their own infor-

mation eliminates the bottlenecks and distortions inherent in running up and down the chain and teaches them to grow smarter faster through experience.

But is using market logic the best way to outfit a military? Markets do not work unless people have something to spend, which raises the question of who starts off with what resources. Even if each unit started off more or less equal (and they cannot because units differ in their needs and readiness), some units but not others will, in the course of combat, need to get or gather new information quickly and often desperately (but if asking for more gets you more, where is the discipline?). Just as commanders historically added value by knowing when and where to commit reserve forces, they will be expected to add value by knowing where and when to commit assets to gather and distribute information. Having unit commanders bid against each other to receive, for instance, UAV coverage, cannot help but yield results that are bizarre from a military point of view (and assumes the military wanted to promote officers who excel at hustling information markets). In commercial life, corporate bureaucracies can often exploit lower transaction costs and shared trust to outperform independent businessmen linked only by market relationships.

Furthermore, the moral fit between market forces and militaries is poor. Militaries are hierarchies for a reason. Command relationships have to be unambiguous. Everyone works for a common goal, not individual ones. The willingness to sacrifice is the hallmark of the organization and, indeed, of its highest virtues: obedience and courage. Selflessness is a primary virtue, whereas selfishness, as Adam Smith wrote, is essential for capitalism. A force in which every man is out for himself is either a marauding mob or one that has been or is about to be defeated. Overlaying the logic of the market atop the hierarchy of the military is no easy fit.

SUMMARY

A theoretical discussion of the competing principles of centralization and decentralization can inform the discussion, but only so far. In practice, specifics—who needs what information for whom and for which purpose—will matter. The next two chapters discuss criteria to be applied to such specifics.

Chapter Three

WHO PROVIDES THE DATA?

Although information systems are more than sensors, without some method of gathering data, there is very little content to work with (apart from what comes from monitors, reports, and news; however, nothing tracks the other side so well). Sensors undergird the U.S. claim of superior situational awareness. Their deployment and operation is a matter of command choices. Their development, placement, maintenance, and constant validation can be resource-consuming; they clearly involve operational units that must often go in harm's way to put the sensor where it belongs. Almost alone among the various components of an information system, sensors have to sit somewhere in the material world. Conversely, because information systems are growing ever cheaper and information is easily replicable, sensors can be commanded and controlled from anywhere at any time.

Consider two approaches to slicing the information pie into global and local pieces based on where the raw data come from. One is to build discrete information systems around each sensor. Each system would provide tools to command and control its sensors, data pre-processing (e.g., orthorectification, noise reduction, semiautomated target analysis), data storage, (software) object maintenance, and basic security protection. Data made clean, interoperable, and secure would then be made available over the Grid: certainly downward to users and, unless otherwise burdensome, upward for broad-scale analysis, lessons learned, and general archiving. Everything else after that is up to those who build networks and provide value-added services.

The other approach develops mission-specific information systems (perhaps better envisioned as information suites or virtual systems). Such systems would draw data from global and local sensors, and the *balance* between the two sources would suggest whether it is better to command and control such systems from the field, from the continental United States, or somewhere in between (e.g., CINC/JTF headquarters).

A SENSOR-CENTRIC APPROACH

Sensors may be differentiated by their coverage, in terms of both what they see at any one time and what they see over the course of their deployment. Generally, the broader the coverage, the more sense it makes to manage them globally and have their services provided to local warfighters. Conversely, sensors with narrow coverage are more appropriately managed and tasked locally.

Global Sensors

Many global sensors operate largely irrespective of who commands them. Their data can be made broadly accessible, and what they produce follows naturally from how they are engineered. One class includes satellites in geostationary orbit that provide signal collection, electronic intelligence (e.g., for ship location), meteorology, early warning, and monitoring of nuclear events. Ground sensors tied into a global network may also be considered global: Examples include weather stations; seismographs (used to detect nuclear blasts); SOSUS arrays (for finding nuclear submarines); over-the-horizon radars; and, more broadly, disease-monitoring networks. Collectively, such sensors form at least a large share of what might be globally provided to warfighters.

A second category of global sensors provides global coverage that varies by command. Surveillance satellites, for instance, can be pointed and "clicked." Electronic intelligence sensors could be tuned to specific frequencies. Sensors in this category may thus be reallocated from national managers to local warfighters and back.

Regional assets are likely to be under CINC or at least JTF control with their data entered into commandwide databases and, from

there, distributed to field units. An example may be a sensor-laden UAV, which, at an altitude of 20 km, can theoretically (and across flat terrain) see almost 500 km to the horizon and 850 km to civilian jet aircraft at cruising altitude.

Local Sensors

Local sensors characteristically have a limited search area and support a mission with a geographically narrow focus (e.g., to help an army company). Ground-based sensors tend to be local sensors (with exceptions noted above). So, too, are sensors mounted on platforms and precision-guided munitions. Local sensors are often deployed by operational units for self-protection and to search out their enemy counterparts. Warfighters are, in effect, local sensors; next-generation personal weapons may also be sensors. So are host-nation allies and trustworthy witnesses (but spies managed by U.S. intelligence agencies are therefore global sensors).

Many local sensors are better understood as feeds into a global database than as stand-alone units. They may capture information on an enemy that can be used to build intelligence estimates on its deployments (for national decisionmakers) and capabilities (for intelligence estimates). A suite of ground-based sensors deployed to warn the world of a conventional invasion will generate information that will concern the unit directly opposite the invading force—and be of great interest well beyond.

The Difficult Global-Local Nexus

Thus, systems fed by local sensors ought to be of local responsibility; systems fed by global sensors ought to be of global responsibility. Systems for which sensors are a minor component (e.g., information operations; see below) may be organized around institutional considerations (e.g., global, if expertise is concentrated; local, if the architecture of the system must be minutely responsive to field commanders).

In some cases, a global-local split is straightforward. Take weather forecasting. Global forecasting uses satellite and local sensor information to fill in a gigantic fluid dynamics model. Local assets, such

as Doppler radar, are used to predict local phenomena, such as the onset of severe weather or the likelihood of wind shear around airports. The former forecasts over days; the latter, over hours. Data from local Doppler radar do not feed into the global model, but the value the global model adds is too generalized to inform the immediate local forecasts. The result is a fairly clean division of labor. Global forecasts are globally provided; local forecasts are locally provided (albeit with assets perhaps acquired or trained globally). Commanders use the former to plan operations and the latter to conduct them.

But then consider missile defense. True, DoD's early warning satellites (and, soon, space-based infrared radars) can detect a launch and even determine an ellipse of probable impact. But this information is only the beginning of a complex coordination of sensors and weapons designed to engage the missile over the few minutes of its flight time. So, should global sensors cue local engagement systems, or should global systems command local sensors?

Sensor Coordination

Is a sensor a camera or a tool set? The latter aspect comes into play when sensors must be coordinated to bring out some aspect of the environment. Some local sensors may be part of a global network whose efficacy depends on coverage and coordination. If local commanders vary in the amount of sensor coverage provided, adversaries who find the weak spots can plan operations accordingly. Just as in any military line, some parts are weaker and thus more inviting of attack than others. Both are phenomena that commanders are supposed to find out and counter through the assignment of reserves. At very least, knowledge about sensor coverage ought to be globally available. When sensors must be concentrated in one place or for one purpose to gather detailed information on emergent phenomena, managers must know where to divert them from and assess the consequences of such diversion.

How well sensor data are correlated may come to matter more than the sensor's individual field of view. Correlation may be necessary to detect a pattern of anomalous activity that foretells enemy action, e.g., terrorist attacks, preparations for electronic warfare, or raids. Some locally acquired information has to be globally accessible:

what corroborates or contradicts intelligence, builds a mosaic on the enemy, stitches together target tracks, provides a history of an area so that changes in it can be detected, crosses domains (e.g., actions of enemy units can inform information operations), or populates a data file from which lessons can be learned and so on. Sensor data collected from airborne platforms can support ground operations, just as electronic intelligence collected by special forces can be used to build a picture of the air threat. At very least, each sensor should be capable of formatting output in standard ways (e.g., for correlation or for fusion) and transferring results to a repository or a processing node. Tools to cross-cue sensors are specifically discussed in Chapter Four.

The more that sensors are deployed in large numbers, the harder it is for people to command them individually and the greater the reason to empower each of them to command one another (especially if tracking fleeting targets against a cluttered background). A spacecraft that picks up a possible match to a target signature may cue a UAV for a closer look. To aid target discrimination, a UAV with its own logic elements may then cue ground-based acoustic sensors to point their ears or to use a particular frequency to pass along their readings. Today, such steps take place through component commanders (e.g., from intelligence analysts to the UAV coordinator of the JTF to a battalion intelligence officer). If coordination is tightly engineered, sensors can collectively be considered a single system. Command over a single system of sensors may move up the hierarchy or it may be reassigned from its normal chain to an ad hoc system created by a team of various information-system providers.

There must also be enough interoperability not only to permit data fusion but also to negotiate queries and/or taskings and responses. How, for instance, does the ground sensor tell the UAV that it cannot collect data as requested—and vice versa? There also ought to be at least one higher assessment center that can analyze such interactions, evolve useful rules for governing them, and provide a clearinghouse from which the results of such interactions (e.g., fused data) can be pulled. Doctrine and the technical aspects of interoperability can be worked off line (i.e., in the long run, they need not be part of the system core); the day-to-day aspects of interoperability may need central management. However, assessment centers and repositories need to be global.

This holds for integrated target tracking. As a potential target crosses from one area of operations to another, relevant data ought to be passed from one local unit to another. Such data can range anywhere from a simple location and movement vector to signature data that indicate why an entity is suspicious. In some cases the entity may be in multiple jurisdictions; a low-flying helicopter may be tracked by both aircraft and acoustic sensor arrays on the ground. The information requirements for data exchange include interoperability, and a mutually accessible repository of information. The first can be done locally; the second is more likely a global function.

Bureaucratic Barriers

Another objection to organizing information systems around sensors rather than missions is that systems imply bureaucracies (to write requirements; develop systems; and provide resources, doctrine, and training materials). If space systems create data that flow through Washington, D.C., macro-UAVs create information flows through CINC headquarters, and micro-UAVs create data flows to the soldier, warfighters who need a consolidated picture will instead get three different flows of information without any good way of determining optimal coverage or asking for it. Worse, such bureaucracies may have different cultures, philosophies, and access methods—even though they serve similar needs.

Furthermore, the existence of and *self-justification* for such a bureaucracy may impede adaptability. As technologies change, the sensor array required to fulfill a task may shift from local to global (e.g., from radar to SBIRS-Low in building incoming missile tracks) or the reverse (e.g., from air defense radar to distributed microphones in tracking aircraft). Circumstances also change: The thinner the overseas basing structure is or the more-sensitive nations are to unmanned flyovers, the more spacecraft may be favored over UAVs. Sensitivity to collateral damage or the ability to react to fleeting phenomena make UAVs look better. New challenges constantly arise—where, for instance, should improvements in targeting accuracy come from? An upgraded GPS constellation may support better weapon accuracy; while expensive, this is a one-time cost. Boosting the local accuracy of GPS through differential GPS emitters may be cheaper for any one mission but requires that emitters be rapidly and

accurately placed, spoof-proofed, and hidden from an adversary who may control the ground. Improving the acuity of weapons so that they may merge less-accurate GPS information with precise knowledge gained from matching the signature of the aim point with a given template adds to the cost of each weapon but is relatively hard against many electronic warfare countermeasures. Arbitrary command distinctions from one information-system provider to the next ought not stand in the way of optimizing solutions to technical problems (as they often do in noninformation fields).

A MISSION-CENTRIC APPROACH

Alternatively, information systems could be built around mission areas (e.g., suppression of enemy air defenses [SEAD]). Missions generate requirements for information, which, in turn, generate requirements for sensor data. The extent to which such sensors are local or global will have a strong effect on whether the information systems for such missions should be run locally or globally. At the least, such systems will be organized to solve specific warfighting problems—even if command and control over the resulting information system sits at an echelon higher than the level at which the mission is commanded.

To see where this notion leads, take a sample of 21 missions: four information operations, five other strategic missions, nine combat operations, and three ancillary tasks—a listing with wide coverage but no claims for completeness. To summarize results from Appendix B,

- Computer network attack tends to be a global mission because of its political sensitivity, scarcity of good hackers, and location-independence. It thus requires a global information system.
- Computer network defense requires mostly local information because it is mostly a subset of system administration.
- Electronic warfare draws from a mix of sensors with global and regional electronic intelligence (ELINT) sensors building a broad map filled in by local sensors.
- Navigational warfare is similar to electronic warfare but tends to have more local components (because jamming is highly localized).

- Defending sites against chemical and biological attack requires local sensors but, because of the mission's political sensitivity, ones analyzed globally.
- Force protection requires a mix of global information on threats and local information for indications, warnings, and incident management.
- Theater missile defense (TMD) is evolving to be a tightly integrated regional choreography with an information requirement to match.
- Military information assistance, with its direct state-to-state ties, is inherently global.
- Border patrol is variously supported by global or local information systems, depending on how intrusions are responded to. Hostile borders favor global information; so do deep frontiers.
- Sea control is moving in the direction of global search mechanisms (except for local challenges to unidentified vessels).
- Fleet air defense, like TMD, is evolving to an integrated local system.
- Air superiority (SEAD and counterair) uses a mix of global and local sensors, and its information support is likely to be an overlaid system.
- Attacking fixed ground targets usually requires a globally managed information system with some local supplementation.
- Attacking mobile ground targets requires more local sensors (including combat forces) and is more likely to be managed through a local system atop a thin global base.
- Close air and artillery support requires modest local information support (knowing where one's own forces are).
- Maneuver is about stealth and evading or overcoming traps. It needs a local information system atop a thin global base.
- Close combat is too quick and too near to use global information (except as background, such as maps).
- Peace operations are similar to close combat but can make better use of limited global information.

- Traffic management is increasingly using local information (witness the Federal Aviation Administration's emerging free-flight doctrine).
- Material management's requirement for global visibility drives it toward a global system, but one locally fed.
- Field medical services are locally supported (helped by forthcoming handheld information and testing devices).

What does this recitation suggest? First, the information systems appropriate for supporting these operations fall all across the board. Four missions appear to be best supported by local information systems, nine by mostly local systems, two by a mixed information system, four by mostly global systems, and two by completely global approaches.

Second, the notion of overlaid information is a powerful one that ought to inform the Grid's architecture. Detailed imagery and other long-term information, maintained in an intelligence database, would be the foundation atop which local data—whether from regional sensors, local sensors, platform-mounted sensors, or soldier reports—would be mounted. Adjunct data, such as the enemy order-of-battle, the politics of the embattled region, and the relevant local information architectures, could use similar treatment, albeit with different topological relationships between layers. General and thus global information is successively modified by local information. The GCCS's common operational picture (COP) permits local and global data to be overlaid because they share compatible coordinate schemes (provided each revealed unique phenomena), but true overlay capability would permit local and global data to be fused so as to modify each other. A single phenomenon that emits local and global signature elements could be discovered and identified by intelligent combination of both.

Third, an analysis of the characteristics of the sensors required for transmission seems to be the right first step in determining whether information requirements should be satisfied globally or locally (intelligence requirements aside). For 14 of the 21 missions analyzed, there was no reason to look further. In four cases, the information system required appeared to be more global than the source of sensors; in each case, the requirement for correlating local sensor

information was considered to be high (but in three other cases, a high need for correlation did not increase information requirements). In three cases, the optimal global information system appeared to be less centralized than sensor analysis would suggest.

Fourth, other factors sometimes affect the overall judgment. For instance, high political sensitivity (as in the case of offensive information warfare or information assistance to allies) emphasizes factors that favor globalizing the mission—and thus the information system that supports it (which is, in essence, the mission). Information requirements are properly influenced by whether a mission serves a local or global purpose. The missions for which this pull appears salient were the protection of cities from chemical and biological warfare and force protection (where psychological issues convert local misfortune into global news). For logistics, the ability to mobilize resources means that local needs benefit from global visibility. Urgency (the less time between observation and action, and the more requirements are shaped by rapidly unfolding events) gives weight to local rather than global sourcing. Close-order combat (firefights and dogfights alike) is clearly a case. Transition-to-war issues, such as TMD and hostile border patrol, exhibited high urgency and global support. Such missions as lift and navigational warfare exhibited low urgency and local support. Overall, the independent factors correlated enough with each other to indicate clustered causality. By contrast, however, the tight timelines of missile defense do not necessarily argue for local control over the information system that would support it. Conversely, the greater the sufficiency of sensor assets, the less important are the details of what they are being tuned to do and thus the less the need for a central allocator.

Fifth, a mission-centric approach comes much closer than a sensor-centric approach to justifying a designated manager in charge of this or that domain picture (e.g., the recognized air picture). The matchup between missions and domains is almost one to one, but not quite. The common ground picture is easily the most critical for warfighting (e.g., for seven of the nine operational missions), but many elements of the ground picture are of greater relevance to other missions. Surface-to-air missiles are of special interest to flyers, just as Scuds are of great note to theater missile defenders. So, a mission-centric approach dominates a domain-centric one.

A mission-oriented approach empowers the information commander to operate whatever resources are needed to present a complete information picture for the warfighter. Inherent in this logic is some ability to switch control over sensors from one level to another. Using such tools, CINCs could take command of fly-over national sensors. Lower-level commanders could get temporary control of theater UAVs (an idea offered by Dr. Louis Marquet at U.S. Army Communications–Electronics Command). Warfighters could exploit heavyweight processing capability in the rear. Field units could tap into expertise to attack local problems on the spot (e.g., experts on conflagrations called together to assess a fire with suspicious characteristics). A corresponding ability for upper-level commanders to pull up the control information and thereby exercise temporary command over lower-level sensors may also be useful.

Of course, this approach can lead to contention over resources. Sometimes this can alleviated by proliferating sensors so that all who need one can have their own—this limits the time wasted in fights. Ultimately, however, people will have to share. They can resolve their conflicts in several ways: doctrine-based priorities, broad authority delegated to lower levels by command, clever artificial intelligence algorithms, very rapid case-by-case discretion by the higher commanders—or a mix thereof. But it may take practice before the right method for the circumstance becomes clear.

SUMMARY

In many cases, the two approaches—mission-centric and sensor-centric—are more similar than different. Both acknowledge the need to provide data from heterogeneous sensors and support systems in sufficient detail and with enough interoperability to be useful far from their collection points (and their collection staffs). In that sense, both also acknowledge the reality that information and information systems are increasingly independent. Both also recognize that "local" and "global" may be continuous and not binary conditions. But the first approach leaves the command of sensors where they started and relies on explicit mechanisms and negotiation to coordinate sensor activities. The second approach permits a single focus for coordinating sensors but leaves sensor allocation as a problem.

Chapter Four

WHO PROVIDES WHICH SERVICES?

Since the Grid is a knowledge base, the choice of local versus global sources for filling it is important. But the Grid also supplies knowledge services, the responsibilities for which need to be apportioned intelligently. Where should analysis take place? How should peer-to-peer knowledge be facilitated and local-to-global knowledge integration be negotiated? How should the Grid be managed as a network? Finally, how large should the core be, that is, what is the proper relationship between the contributions of various global providers?

WHERE SHOULD ANALYSIS TAKE PLACE?

Historically, those who generated a stream of data owned it. They exercised whatever prerogatives they deemed fit to organize, categorize, and analyze the data and forward the resulting information "product" on whatever terms prevailed. If analysis was a high–value-added product, its responsibility rested with the institutions that generated the data.

But how strong should this link be? What can be pushed forward to the user (directly as an analyzer or indirectly as a customer of third-party analysis)? If there is a very close relationship between how analysis is done and the choice of what data are collected to support it, the two activities must be linked. In some cases, such as photointerpretation, the existence of a close-knit community composed of exquisitely trained analysts would also support close coupling between data tasking and analysis. Yet alternatives exist. Analysts could be assigned to local units. Analysis could be considered a

value-added service that can be asked for (and "paid" for?) by the units that would get the raw data. It may be done anywhere if certain conditions are met (especially automatic processing, commercial-off-the-shelf equipment, sufficient communications, adequate in-theater storage, and resolved interoperability and security issues). And human analysts, unless on call and wired in, are unlikely to be used in any operation timed in minutes and seconds.

Whatever economies of scale exist in analysis would argue for concentration (analytic shops do not have to be big, but they do have to bring many if not most of the right people together). But concentration does not mean centralization (much less automatically limiting analysis to the original data providers). With computer-driven analysis, location is nearly irrelevant; software and even fairly large databases can be replicated and sent where needed. Only some analyses require banks of expensive processors: analysis of synthetic aperture radar (SAR) returns, meteorology and other fluid dynamics, and residual code breaking. Even then, if pipes are fat and urgency is low, analysis can still be viewed as a value-added function in the system. The same rule holds for human analysis. If general intelligence functions are conceded to be a global function, on-the-spot analysis of ongoing events could also be supplied as a value-added service over the wires.

Quasi-market mechanisms may permit centers of analytic excellence to emerge on their own. A user could contract for analyzed data (or analyzed data services) under the assumption that the Grid can shuttle the raw data in and the finished data back out. That would leave some DoD (or DoD-sanctioned) entity charged with creating annotated directories of providers, performance standards, data standards, and rating mechanisms for such analyses.

INFORMATION SERVICES

Today's world of independent users and producers pales before the potentially rich set of services that a fully outfitted Grid could provide. It may not necessarily be up to one global provider to provide such services, but determining the requirements for such services, ensuring that they are provided at a sufficient quality, developing the technology to enhance them, and making them secure and interop-

erable are all tasks for which someone must, at some point, take responsibility.

This section discusses some of the more important services that cross warfighting lines (and for that reason are candidates for global provision). This list includes tools for peer-to-peer coordination, information validation and reconciliation, knowledge routing and news feeds, and application hosting.

Peer-to-Peer Coordination

Information on one's own forces and plans has traditionally been of a piece with command and control. Status data floated up the chain, with information consolidated as it rose; plans skinnied down the chain, with tasks hierarchically decomposed. These chains were largely kept within single Services. Even today, Service lines tend to be crossed (e.g., one Service's commanding units from another) largely toward the top (e.g., at the JTF level) rather than the bottom of the hierarchy. Hence, the information systems necessary to coordinate activity have traditionally been supplied by the Services, except at the very top of the command hierarchy.

Several factors are now calling this neat division of labor into question. The pressure for jointness (and the ever-expanding, and thus overlapping, operational footprint of combat units) could result in a finer granularity of inter-Service mixing (e.g., at the Army captain rather than brigadier general level). The finer the granularity, the more points of cross-Service tangency, and the greater the need for deconfliction and interoperability—and thus the more often that service-specific command and control systems have to work with each other (or yield to joint command and control systems). This holds double for coalition operations. Second, horizontal coordination may take over functions from vertical command. The latter tends to be ponderous and inadequate for agile operations. Communication technologies in the hands of networked adversaries (e.g., loose coalitions of like-minded actors) may permit them to coalesce and disperse faster than forces, awaiting hierarchical command and control, can react. To the extent that horizontal coordination—sometimes known as swarming—is broadly effective, it requires that each unit know the status, intentions, and plans of its counterparts.

A system that can elicit, organize, and present information on the status of one's forces requires investment in the requisite capabilities (including real-time collaborative planning), standards that permit such information to be acquired seamlessly, and doctrine that persuades units to keep the knowledge base reasonably current.

Going further, coordination among peer units works better when each understands how its counterparts think (à la Nelson's "band of brothers"). A unit commander given the tools to look over the shoulders of his peers on the battlefield (or in training) may reap dividends in terms of intuitive understanding. Getting such capabilities may require global providers for fundamental engineering, implementation support for client systems, and some hosting of server functions.

Validation and Reconciliation

How much a user trusts the quality of someone else's information is key to its being used. Requirements for information to cross unit boundaries may arise from overlapping functional responsibilities (e.g., both operational and intelligence units are at work there), one's own movements (e.g., air base security units taking over from the ground units that took the terrain), enemy movements, or the need to draw general lessons from consolidating specific events.

Exploiting data requires users, first, to know the data exist (e.g., who has covered the topic or been there before) and, second, to be able to judge their reliability (e.g., whose judgment based on which data). If assessments from various sources are in conflict, users should not be left with one view because they did not know of others. At a minimum, therefore, there should be standards that govern the formatting, pedigree, and filing of locally generated reports.

Users, at best, ought to have—in rough order of importance—search services or directories to find such reports; tags that indicate whether conflicting or confirming reports may exist; rating services that assess the quality of the report; and, perhaps, reconciliation services to find common ground or split the differences the right way. True, only a small fraction of all information will merit comment one way or the other, and even correct content-based tagging may be a hit-and-miss affair. Whether someone is charged to ensure that important material is externally rated is a separate issue.

All these may be considered global services, at least to the extent that they (or at least templates for them) have to be established within DoD.

(Un-) Common Knowledge

But what if people do not know what it is they do not know? Much of an enterprise's knowledge base consists of bits and pieces of knowledge scattered in this or that head. Consider the bombing of the Chinese embassy in Belgrade. Many U.S. embassy employees had been to the Chinese embassy and thus knew where it had moved to—but they did not consider that military planners might know otherwise. Planners did not think to ask embassy people where the Chinese embassy was because the planners did not believe that an embassy was at risk (since their maps showed it to be miles away from the point of impact). But had each shared their knowledge and intentions, the error would have been quickly discovered.

Is there a systems version of cocktail parties or go-betweens that would help bring random needs and knowns together? Computer scientists have envisioned tools that would permit people to dump what they learn to a mass database effortlessly and immediately (speech recognition would help), organize such information by category, and permit a profusion of software agents to mix and match needs and knowns endlessly in hopes of catalyzing a reaction. Should such services prove useful, the case for a central repository (or well-recognized index to a distributed set of repositories) of information collected, organized, and sifted through may be worthwhile—another global service.

A more deterministic approach to mating new information and extant requirements is the publish-and-subscribe method. Users indicate their information needs (or have such needs indicated for them based on their mission), which are then posted to news servers. Whenever an item appeared that was of interest to the user (e.g., a surface-to-air missile lighting up) by such criteria, it would be forwarded straightaway. Making this work requires standard methods of expressing information needs and tagging material and perhaps some technology demonstrations and prototypes. Someone may have to see that the system works as advertised (e.g., are requests getting posted to the right servers; how are new servers stood up?)

and with sufficient participation (without which, people will stop tagging material or posting requests). Such a system has obvious effects on network performance (badly constructed requests could flood the Grid) that must also be managed.

SYSTEM MANAGEMENT ISSUES

Even if most of the information that DoD needs is locally provided and consumed, the global networking to enable command and control and share global information establishes some requirement for global system management.

Network Management

Satellites, long-haul fiber, and bulk switches are necessary elements in a global defense infrastructure, one largely provided by DISA. If and as DoD shifts its traffic over to commercial infrastructures, some central contracting capability may also be required.

Beyond that point, how much global network management does DoD need? Its requirement for assured connectivity (e.g., in the face of electronic warfare), its sensitivity to security concerns, and the surge requirements from unforeseen military contingencies mean that some functions cannot be outsourced. More of the ".mil" domain of the Internet is disappearing behind firewalls. The MILSTAR communications constellation and defense support satellites are likely to remain in DoD hands for years to come. Even DoD-leased gateways owned by commercial providers have to be paid for, managed, and allocated consistently.

Network management entails governing traffic flows so as to minimize congestion, enabling the highest-priority services to get express lanes, and guarding against systemic information warfare attacks (e.g., on routers). When surge requirements push against capacity constraints, central management may be necessary to divert less critical messages into the slow lanes or at least force them to compress themselves to lighten their load on the overall system.

Security management is also necessary if entities within defense perimeters are to trust each other more than they trust those outside. Thus, there must be some standards with which to rate the compe-

tence that DoD components exhibit at security management, and someone has to do the rating. Public-key infrastructure management may also be a centralized (or at least a federated) function.

Tool Hosting

Big servers in the rear may have a useful role in the Grid. Some analytic and service tools are better kept on servers and distributed in bits and pieces as required rather than shipped as shrink-wrapped software. Likewise, some queries are better run on large databases with the results passed forward, rather than having the clients download the data themselves (especially over thin connections). Given the tendency of software to grow without limit, even Moore's law cannot guarantee that all fat applications will migrate to thin clients (especially handhelds) in the field. Server hosting also ensures that everyone is using the same version of the software. Finally, if, at some point, complex software improves with use (e.g., neural nets, knowledge engineering programs capable of learning), central management ensures that, as the cliché has it, the experience of each becomes the wisdom of all. Furthermore, some DoD applications, especially those that permit collaboration, may have to be centrally acquired and distributed widely enough so that people can rightfully expect to use such services wherever they are. Uniform applications, for all their drawbacks, at least permit standardization; this is one reason they have become part of the GCCS philosophy.

Allocation Management

Allocation management is another component of network management. Some forms of control exist today: spectrum allocation at both the local and global (e.g., satellite) levels, flash-level prioritization for message traffic within capacity-limited networks, and the implicit prioritization of service that comes from giving military rank its due.

The ability of one individual to flood the screens of literally millions of others within DoD suggests other requirements for prioritization. What messages, for instance, would automatically insert themselves at the top of a user's screen? Should this decision be made centrally, by the user, or through a user-selected service that rates messages by

content and sender? As another example, the transmission control protocol–Internet protocol (TCP/IP) assumes that every user's system cuts back its own transmissions when it encounters congestion; if cheating erupts, the system breaks down and some central authority may have to reserve clear lanes. If applications are posted by third parties on the Grid, there may have to be rating services that indicate that they are network-safe to deploy and client-safe to exploit. The ability to task sensors not under unit control, as hinted at earlier, is another area in which privileges—"tickets"—may have to be allocated.

Developing the criteria—or at least negotiating a set of reasonable and transparent algorithms—for handing out tickets is a core function; so is handing them out or devising a federated system to do so without excessive contention.

Standards and Cross-System Access

Integration (or at least integration without some czar) requires putting considerable effort into standards. Such efforts have to continue as long as technology keeps changing, which is to say indefinitely.

Generally, if DoD adopts commercial standards, it need invest only modest resources in their adaptation and refinement. DoD may want interim standards in areas of special concern, such as security, or for enterprise management issues, such as code reuse, that are problematic as the number of system nodes crosses a million. Because the domain of military operations is unique, it will also need semantic standards (i.e., how to refer to the same item or class of items in the same way) to accompany nascent grammatical standards, such as the Extensible Markup Language (XML). DoD's message and data standardization initiatives are one thrust; earlier work on defining structured text for DoD's Computer-Aided Logistics Support program is another.

The adoption of commercial standards, however, does not mean that all other engineering efforts on the Grid are finished. It takes work to determine when standards are mandatory, to stay current enough with standards to sense which ones are likely to end up being widely embraced (as others fall into disuse), to select enterprise profiles for

standards with multiple options, and to devise (or adapt) test methods for interoperability. And getting everyone to follow the standards on which they had supposedly agreed is no small task either.

Standard methods of access mean little if access is otherwise denied. There must be constant checking and advocacy to see when valuable sources of otherwise obtainable information are not overly restricted because connectivity is limited or information is overcompartmented. If people are given responsibility for providing information, applications, or rules of thumb (in some future distributed knowledge-engineering system), their contribution has to be both reliable and timely.

The more globally accessible information, services, and tools are, the greater the incentive local users have to invest in connectivity, open up their systems, and adopt standard methods to exploit them. Having made such investments and perhaps having seen the benefits of data sharing, users may more easily accede to making their own information easily and readily available to their counterparts. This factor alone argues in favor of global rather than local responsibility for certain functions when the data may be of use to others. Likewise, the more resistant local providers are to sharing information with their counterparts, the stronger the rationale to pull such information into the core.

HOW LARGE A CORE?

The growing list of responsibilities for information management that *could* be globally managed or at least made globally accessible leads to a key question: Do all global elements need to be managed as a whole by the same entity?

Today, global providers are, as noted above, scattered throughout DoD, largely in defense agencies and notably in the intelligence community, but with DISA and the Defense Logistics Agency (DLA) playing large roles. Coordination among such agencies falls short of perfect but is by no means the most troublesome of institutional seams within DoD. Networking should facilitate coordination; it is also easier for one agency's user to sift through the files of another than to ask explicitly for data to be actively forwarded.

The options for coordinating global functions range from doing everything by hand (i.e., the status quo), to appointing a champion (or at least someone to coordinate information flows) for specific called-out functions (e.g., painting the global COP), and to anointing a czar (whether a person, an entity, or a board of governors) over the Grid. DISA, with its responsibility for long-haul communications and its evolving GCCS and Global Combat Support System (GCSS) suites, is clearly the most obvious global provider, but its resources, credibility, and clout pale beside those of its intelligence counterparts. Its reputation even within the community of information technology specialists is by no means uniformly sterling. However, with the intelligence agencies forced to shift their focus from the president's ear toward the warfighter's palmtop, a future DISA may be in a better political position to get on top of the information pile.

But should it? Despite all the efficiencies of a single core provider, DoD has to be nervous about centralizing *all* global information functions. Error or bias present in the core provider has little natural correction. If the core errs, it can fail spectacularly. Of no small risk is a core that diverts more and more of its effort into ensuring that the core's viewpoint is dominant and suppressing all others.

Good military sense dictates that those who run the core not make decisions that the CINC can make. That said, if interoperability, for instance, is made impossible by the choice of hardware or software brought to battle, the CINC's hands are already tied.

So, what is the minimum that a central global provider should do? Primarily, DoD functions that normally come under the aegis of a central information officer need to be integrated—system administration writ large:

- *Interoperability*—Until that ever-receding day when translators can effortlessly convert bit streams from incompatible systems, some standards will be necessary, and the core has to certify what are to be followed—and no more.
- *Security*—DoD needs a single service through which parties to a classified transaction can authenticate themselves as having certain privileges and can vouch for the security of systems and their owners (such a process may have to be extensible to

alliances, such as the North Atlantic Treaty Organization [NATO], or partnerships).

- *Advocacy, Trade-Off Analysis, and Certification*—Because sensors and bandwidth cost money and because their benefits are spread widely, owners of each may not necessarily provide sufficient coverage (in time and space) or connectivity. The core should not only set the *de minimus* standards for such services but also be able to argue why they are worth funding. The core should also be able to check on whether owners have provided the capabilities they claim to—and whether they can be accessed fairly. Again, such a function can devolve to CINCs for theater-level assets.

Honest advocacy of a minimal core has to acknowledge that standards and persuasion may go only so far in facilitating coordination. If they fail, some global functions may have to be moved into the core.

Finally, it is worth asking: How does the marvelously acentric Internet manage such functions? Such institutions as the Internet Engineering Task Force and the World Wide Web Consortium do a decent job on standards. They also illustrate that a simple networking-cum-presentation core can permit a variety of services to thrive because the complexity is pushed outward to where it can evolve without requiring systemwide adjustment. Yet, DoD's requirement for standards goes beyond what can be borrowed from the Internet. Although market forces have impelled a profusion of information sources and conduits and manage resource contention, market forces are attenuated or absent in DoD. Meanwhile, weak security, the difficulty of separating wheat from chaff, and guaranteed quality of service remain sore spots for the Internet.

SUMMARY

Two functions belong under global management. One is to provide global information. The other is to create standards, engineering, and some facilities for conducting inherently core functions, such as hosting peer-to-peer interactions and system management. But not all global functions belong in the core. It suffices that they be done in an interoperable and mutually accessible way. To the extent that

pluralism is institutionally desirable and that the performance requirements can be stated succinctly for such tasks, they are better off devolved.

Chapter Five

CONCLUSION

What military information should be a global responsibility to provide, and what should be local? Empower the global producer and reap coherence in the information domain. Empower local consumers to get their own information and see a tight fit between the demand for and the supply of information. This tension is inherent in modern warfare, but the dilemma can be reduced through a strategy that (to echo Air Force doctrine) may be described as "centralized architecture, decentralized services." This strategy recognizes that data originate with sensors and thus those who control the sensors but that analysis and integration need not originate there as well. The purpose of such a strategy is to enable CINCs and subcomponent commanders to create whatever information picture they need. To do this, it is necessary *first* to standardize and make accessible information sources within DoD (centralized architecture) and *second* to develop a set of tools (which work together) that users can employ to manage these information sources and to build their pictures (decentralized services).

It is important to understand what this strategy does *not* do. It does not necessarily advocate collecting (or processing or transporting) information using other methods (e.g., shifting from spacecraft to UAVs). Neither does it advocate shifting responsibility for acquiring and/or operating information assets from one institution to another (e.g., from the NRO to the Air Force Space Command). What it does advocate is a different way of architecting and providing services for the Grid so as to permit more freedom in matching the command and control of information to operational exigencies.

The logic of this position is presented in two parts. The first part recapitulates the various lessons from the prior chapters. The second part lays out the recommendations in greater specificity.

RECAPITULATION

Previous chapters, if nothing else, demonstrated that there were no easy answers to the problem of what should be provided globally rather than locally.

Chapter Two laid out the basic conceptual rationales for both the global and local provision of information. Both have merits. Global provision promises efficiency; local provision promises responsiveness. All-global or all-local information systems are a fantasy as long as some functions are inherently global (e.g., staring sensors from space) and others are inherently local (e.g., the tacit knowledge warfighters gain from operations). Even the distinction between global and local has to accommodate regional (e.g., information from assets directed at the CINC/JTF level).

Chapter Three, which looked at the relationship between the scope of a sensor and its command and control, reflected the *prima facie* tendency for collection assets, rather than transmission or processing assets, to drive the global-local orientation of the overall system. That noted, the responsibility for creating an *integrated* picture of the battlespace depends not only on the sources of the component data flows but also on how the flows are tied together. The missions in Appendix B indicate how greatly information requirements vary from one mission to another: Some tend toward the global, others to the very local. Information provision is a layered construct. The bottom layer consists of data and services that global systems provide and that collectively create a received global picture. Atop it are inputs from CINC/JTF-level assets and systems, capped by information from operational field units to complete the picture. The result may be likened to a map composed of successive acetate sheets. Powerful fusion, presentation, and annotation services are implicit in this picture.

Chapter Four emphasized the growing role of support services within the information mix. Some services are useful for coordinating local information (e.g., sensor data, lessons learned) to create a global pic-

ture. Other services, such as network and security management or directories, are required simply to keep everything functioning.

Overall, generating a synoptic picture of the battlespace requires information sources that (1) receive the incoming data and (2) output them in readable chunks to (3) a network that sends the data where needed, so that they (4) can be fused with other data and otherwise processed and (5) can be made available to decisionmakers and operators—who may in turn levy further requirements on information sources. This is simple to state. But what does all this entail?

RECOMMENDATIONS

The overarching goal is to help decisionmakers, wherever they sit, assemble the information picture they need from whatever sources exist.

First, there must be a strong bias toward interoperability within DoD, reflected not only in Pentagon decisionmaking on programs but also through the creation and enforcement of a supporting architecture. This bias is already emerging; it needs to be strengthened.

Interoperability, in this case, means that data (largely but not only sensor data) should be put out to the universe (of legitimate users) in transparent format and with no more processing than necessary (i.e., cleaned but not necessarily fused before others can look at the data). Bandwidth (and emission) constraints, as well as interoperability and security considerations, are often put forward as reasons for not doing this today. Yet, technology can be pressed into solving the first, and the rest are often excuses.

To develop and enforce a good *open* architecture, DoD needs an agency that is smaller, is more focused, and has higher stature than DISA. Such an agency would examine and resource the requirements for greater bandwidth (*from* rather than just *to* the field) and would measure the progress of Service-based systems against the next-generation Joint Technical Architecture (which, at a minimum, comports to the Net and the Web).

Second, DoD programs should exhibit a preference toward local control of information sources. Technical requirements being met (e.g.,

sufficient acuity if coverage is to be useful), sensor coverage has its advantages (e.g., many cheap UAVs, while less efficient, may be more usable than a few expensive UAVs). This would cut the likelihood that commanders are blind because they cannot get the allocation of sensors they need. But it also creates the need to think about command and control arrangements for integrated meshes of sensors too numerous to be managed individually. A similar bias should hold for bandwidth: Buy more fiber, even at the risk of having to go back to satellites should disruptions occur. As noted in Chapter Three, warfighters from the CINC down need tools to be able to call for, get control over, and manage information sources on a spot basis—even if for only a few minutes at a time.

Third, more technology is needed for new ways of integrating local and global information by making it easy to overlay local information atop a global tableau. Such a capability requires the development of seamless techniques to rapidly correlate data coordinates; accommodate uncertainty in locational information; conduct spot fusion; and permit a wide suite of annotation, feedback, and manipulation tools. Further research may be needed to support overlays in information realms not suitable for map display.

Fourth, DoD needs an entity that would (1) assess the suite of tools and systemic services already provided through the Grid, (2) draw up requirements for new or improved ones, (3) nominate a provider for them, and (4) monitor their development. Since no such tools and services will come free, approval of step (3) has to be coordinated with the planning, programming, and budgeting process. But the other steps are essentially analytic functions.

At a minimum, DoD should review current globally provided information systems to ensure that the overall suite includes

- intelligence about the doctrines, equipment, and intentions of allies and adversaries (with appropriate pedigree but not sources and methods)
- the COP, as composed through the use of national-level sensors
- the global availability of logistics and lift
- systemwide services, such as at least one good directory and search mechanism, reachback to expertise, network manage-

ment, and security authentication (together with a coherent set of rules for access controls)

- applications, knowledge bases, and analytic services too large (or too real-time) to be hosted locally and too important to be left to lower echelons to develop, engineer, and maintain.

Part of this assessment process entails looking at whatever tools and services are being deployed at the local and usually bench-scale level (as well as within the commercial world), evaluating their usefulness, having the winners scaled up for broad interoperability and widespread (i.e., meganode) deployment, and making them available. Availability means getting the word out on their existence, finding a host for them, working their characteristics into a global directory, and encouraging the development of training materials. If data flows are well-formatted, value-added services that exploit or enhance them need not come from the original data providers. Outside services could add value to globally provided data as easily as they do on the Internet. If DoD is nervous about its services coming from anywhere, it may establish some seal-of-approval mechanism for them—as long as decisions on approval are expeditious. Of course, such value-added services should themselves import and export information in transparent and open formats.

Applicable tools may be those that

- help gather local news with strategic import (e.g., attacks using weapons of mass destruction, border breaches) for national-level decisionmakers
- compile and help maintain good archives of lessons learned and frequently asked questions
- organize bit flows fed to allies
- coordinate local sensors (as opposed to the sensor readings themselves) and at sufficient detail for *long-range* weapon targeting
- describe blue force layouts: location, status, intentions, contingencies, and plans.

The tough nut in all this is persuading lower echelons to forward data to global or regional systems. Regional systems at least can be fed by

levying requirements through the chain of command, starting with the CINCs (if they so choose—otherwise, why bother?).

Should the agency that supplies the architecture also be the one that supplies the services? True, services imply architecture. If DoD were to run a tailored news-feed service for individual warfighters, it would need to persuade people to contribute news items and label them in standard ways. Changes in data formats have to be brought before those who design the services that use the data. But architects and service providers reflect different cultures. Architects inhabit a top-down culture, which promulgates standards and develops conformance mechanisms. Service providers inhabit a bottom-up culture, which scans the world for what is bubbling up, finds ways of making its discoveries broadly available, and can help a broad spectrum of users.

The four recommendations, combined, can put more power in the hands of users. If information flows are interoperable, if tools (e.g., for overlays) exist for manipulating them, and if sources are distributed rather than concentrated, the ability of all users to see the battlespace as they need improves. The CINC especially should be able to command all the resources needed for an integrated battle picture.

SUMMARY

So, should the Air Force be responsible for providing all warfighters with common situational awareness? Clearly, no. At a minimum, no one Service should be put in charge of anything so central to the others. But the same answer holds even if the entity sits above the Services. First, the components of this awareness range from global to local, and in no simple way. Second, complexity mandates that the integration of such information be loose and thus standards-mediated, rather than tight and thus engineered. Third, the flow of information up or down cannot be prescribed in advance but varies from mission to mission and from CINC domain to CINC domain.

But just as clearly, some entity has to be in charge of architecting the long-haul communications and setting the connection rules—and these connection rules only start with the Joint Technical Architecture (whether the entity acts more like a coordinator or more like a

commander is a separate issue). As noted, some entity ought to oversee the mix of services that comes with the Grid to plan the acquisition of future ones.

In the end, the case for making the tools as flexible as possible so that they may assembled at will in various combinations rests on the cliché that the future can only be guessed at and on the repeated discovery that guesses are often wrong. Thus, the ability to adapt to the next war is more important than any efficiency at accomplishing well-defined tasks of past or even imagined wars. No rigid information architecture survives contact with the enemy. In this business, there is no such thing as having lived happily ever after.

Appendix A

GLOBAL PROVISIONING OF LOCAL EQUIPMENT

The case for global provisioning (e.g., a joint program office) or at least global specification of local equipment revolves around issues of economics and interoperability. Questions of responsibility or command and control are far less relevant.

A good example of global provisioning would be the GCCS, which is a software suite that provides the COP and access to messaging, planning, and mapping tools. DISA has contracted for sequential builds of the software, which are currently distributed to thousands of workstations among the CINCs, the Services, and support agencies.

Global provisioning has several things going for it. First, interoperability, particularly across Services, but even within them, would likely be better. Today, even long-standing communications functions, such as voice, present difficulties (e.g., U.S. Marines cannot talk to NATO except through U.S. Army translation equipment; secure voice is problematic among aircraft). Fortunately, the advent of the Internet means that many aspects of equipment come standardized from the civilian world. But data are often difficult to exchange unless two entities use the same database. DoD's efforts to normalize data element definitions is honored only in the breach. Applications that should be able to exploit each other across equipment are almost nonexistent. Security regimes that cannot interoperate either leave people disconnected or, if papered over (often the case in emergencies), leave holes for enemies to exploit. Limiting user discretion has other advantages: Training materials and user support are easier to provide; interoperability can be greater; and the opportunity for security breaches is reduced.

Second, costs should be lower. Having each Service support multiple systems means that services and applications that should be common to all must be duplicated for each owner. In effect, the same work has to be done multiple times, and there is not enough work to permit multiple vendors to compete with each other. Each user faces a vendor with a temporary monopoly, which not only permits the vendor to charge a pretty penny, especially for contract modifications, but encourages this behavior because of the lack of long-term relationships to nurture. When similar costs must be borne repeatedly, some functions become too expensive, and the result is a patchwork of poorly kitted networks when economies of scale could permit the development of advanced software and services.

Third, to the extent that such equipment is expensive or specialized, having one provider could make it easier to justify overall resource allocations. C^{4}ISR resources channeled through a global provider could be mapped into capabilities, which could be compared for their relative cost-effectiveness. Channeling resources through multiple local users does not permit cohesive determination of what overall information capability has resulted.

Fourth, Grid services that require a critical mass of users before they pay off may be stymied if the high cost of reception equipment deters initial customers. Subsidized (or free) distribution of the requisite equipment can kick start a system. Providing workstations with preinstalled software is currently a means for global organizations (e.g., the NRO) to equip warfighters with special capabilities.

But none of these arguments is without counters. Standardization, for instance, is often purchased at the expense of flexibility. For example, users of the COP cannot manipulate data in ways not specifically engineered into the system. Those wanting specific data elements displayed in particular ways had to apply for an engineering change in the software build—a process that, at best, takes months and years. With more complex software that involves desktop analysis and decision support, users may want more-sophisticated services: the ability to alter algorithms that determine how sensors are fused or how news feeds are filtered, a different training regimen for systems that learn through knowledge engineering, or alternative business process logic for sensor management. The more efficient way to achieve standardization is to restrict the requirements for interoperability to the interfaces that connect the system

to the Grid. It does require that system designers be explicit and precise about what these interfaces are, but this is an exercise worth going through in any case.

The cost argument cuts both ways. Part of the problem is the way expensive development costs for software are allocated over units purchased. Software (or worse, software-equipped workstations) is expensive, and buyers whose needs differ from each other have less incentive not to duplicate development costs through a separate purchase—after all, they would have to cover them one way or another. Economic theory would have development paid for outright and distribution made very cheap. This creates an incentive for every subsequent user to leverage the original development expense, choosing only to pay for further development to serve unique needs. The problem with having everyone buy into one development is that the requirements for the system at issue tend to escalate to cover everyone's uncosted wants as well; this raises software costs, the requirement development lead time, and system integration expenses. This is one reason why the Navy's large Computer Aided Design II purchase was not a multi-Service program—getting the Navy's five systems commands to converge on one statement of requirements was hard enough.

The counterargument on coherent requirements echoes that of the main text: Is it better to have a coherent rationale for DoD's overall C^4ISR architecture or for Service-purchased warfighting systems of which C^4ISR is a part? The answer may be that the former is growing in importance, but exactly when it becomes more important will vary.

Finally, although the "infant capability" argument for subsidizing equipment retains economic validity, it can also cover up the bad investment decisions of global agencies foisting systems of low value on local users who do not object because they need not pay.

If there is a resolution of these pros and cons, it probably lies in (1) addressing interoperability directly with standards, technology, and testing, rather than indirectly with acquisition; (2) moving to marginal cost pricing for developmental software; and (3) solving the analytic issues separately.

Ultimately, the issue of who provides local equipment and who provides local information coverage is the question of how much license users are given. The fewer options that users get to exercise, the more that a local system looks and feels like a global system and the fewer the advantages that can be realized from making a system respond to locally unique needs. Global priorities can be built into systems through excessively specific requirements as much as they can by having the command and control exercised from outside the theater.

Appendix B

TWENTY-ONE MISSIONS ANALYZED

To support Chapter Three, this appendix reviews a selection of 21 major missions in four areas: information operations, other strategic missions, combat operations, and combat support. For each, the discussion asks: What is entailed in the mission? What information do warfighters need? How would they get it? And where (on the local-global continuum) should it come together and be managed?

The dependence of missions on long-term intelligence (and thus on intelligence-handling systems) is *not* discussed because, as Chapter One noted, such information has traditionally been provided from global systems, and there is every reason to believe that this will continue.

INFORMATION OPERATIONS

The four missions discussed in this area are computer network attack, computer network defense, offensive electronic warfare, and its cousin, navigational warfare. Table 1 summarizes the missions and the key parameters that influence whether supporting information is better sourced locally or globally (general intelligence aside).

Computer Network Attack

Computer hacking can be used to degrade, spoof, or exploit target information systems. Most such attacks require some intrusion (whether from without or, through subornation, from within) into the affected systems to assume unwarranted privileges. Success

Table 1

Summary of Parameters for Information Operations

	Sensors	Correlation	Purpose	Urgency	Other	Thus,
Computer network attack	Global	No	Global	Low	Politically sensitive	Primarily global
Computer network defense	Local	Yes a	Local	High	Economies in tools and training	Moderately local
Electronic warfare	Mixed	Yes	Local	High		Moderately local
Navigational warfare	Mixed	No	Local	Low	Fixes may be local or global	Moderately local

NOTE: In this and all subsequent tables, *Sensors* are either global, local, or mixed, depending on the type supporting the mission. *Correlation* is "Yes" if it is necessary to use multiple local sensors for signatures that are below the threshold of a single sensor. *Purpose* is either global or local, depending on who shapes the specific requirement for information. *Urgency* is "High" if the information is needed for immediate operations (i.e., within a few minutes). *Other* is miscellaneous commentary. The last column provides a net judgment about where the requisite information falls in the global-local spectrum.

[a]For indications and warning.

requires prior knowledge of opposing network architectures, but intrusion itself will build such knowledge and will permit devices (such as network monitors) to be implanted in the target computer to generate future flows of knowledge about opposing network architectures. Attacks, such as spreading viruses or flooding networks, tend to be blunt instruments of modest military utility.

Offensive computer hacking tends to be an activity for which national-level coordination is critical (in part because its legitimacy is poorly established). The population of really good hackers is small (and thus hard to distribute among CINCs, much less lower-level commands). Empowering mediocre hackers to fiddle around may warn the enemy that something is coming and decrease the total harvest. Both the intelligence and conduct of hacking are independent of location. Some on-site access to target systems helps, but such specialized operatives can be dispatched from anywhere. Some bytes may be inserted into radio-based networks from UAVs or spacecraft but only into systems with poor encryption and with omnidirectional receivers.

Is local information needed to make computer network attack responsive to the unique needs of local commanders? Well into the foreseeable future, offensive hacker warfare is likely to be opportunistic rather than deterministic (and will, in any case, require extensive surveillance of the target system, thereby making rapid response to emergent requirements difficult). Thus, what hackers can achieve and whatever urgent requirements they are tasked with are only weakly related.

Finally, should hackers operate as part of the overall military information system? Hackers can use networks to receive intelligence and tools. But even the merest possibility of blowback and traceability suggests that the hackers be off DoD's networks when on the attack.

Thus, the information to support offensive hacking can be characterized as location-insensitive intelligence—and is therefore best managed globally. The actual hacking itself is probably best done totally off the Grid.

Computer Network Defense

Defending DoD's computer networks against attack would, at first glance, appear to be a systemic and thus global responsibility. This certainly holds for architectural decisions (e.g., setting the security standards). But responsibility for and information collected on defended systems depend on who does system administration, an activity that is mostly local—and perhaps especially so for network security. First, physical access to machines matters for such activities as biometric or device-linked authentication, managing unerasable removable media, or taking a system off line to recover it. Second, imposing and enforcing proper computer usage (e.g., guarding one's password, exhibiting netiquette) is a subset of personnel management and is thus an aspect of local chain-of-command activity.

It is possible to centralize some aspects of system defense, such as the dissemination of indications and warnings, new technology, test suites and tool kits against emergent threats, or the management of expertise for red-teaming (attacking) and blue-teaming (consulting on) systems. Yet, news and tools still do not remove the essential responsibility for protection from local system administrators who must make the day-to-day system configuration, access control, and network management decisions. Local responsibility also promotes a healthy compartmentation so that local faults do not lead to global failures. The less global control there is, the fewer assumptions any one network can make about the benign nature of information coming from another. Indeed, the larger the system is, the more likely it is that there is a sufficiently malicious insider among its users who, if given complete run of the place, can and will take the whole thing down.

The need for global standards on security is clear; being complex, they should not be developed more than once, and the same holds for test methods. A global public-key infrastructure is necessary for authentication if users are to access global information bases (e.g., imagery) or even only deal with their colleagues outside their own work group.

Thus, although there are useful global functions to be performed in computer network defense, most of the information to defend a system has to be local as long as system administration is done locally.

Electronic Warfare

Electronic warfare exists (1) to confound adversary communications and frustrate their radars, (2) to keep one's equipment from being confounded by enemies, (3) to fool adversary signals intelligence, and (4) to exploit signals intelligence on the adversary.

Given global intelligence (e.g., characteristics of adversary emitters), the most important information is the electronic order of battle. Readout can come from multiple sensors: satellites, ELINT UAVs, or listening posts. For the most part, signals intelligence is to be globally reported (except for real-time operations, such as defending a strike package). As for processing, although Moore's Law may permit more local signal processing in the field, the advent of high-capacity reachback, the growing complexity of the radio frequency environment, and the increased sophistication required for tomorrow's electronic warriors may push it to the rear. Correlation between signals and other signature data (e.g., optical, infrared) may also call for the digital equivalent of all-source analysis and hence a global approach. But operators (e.g., F-15–Rivet Joint team) looking for fleeting targets may want to fuse locally acquired information onto a globally provided laydown for rapid response.

Thus, offensive electronic warfare is likely to require a mix of global and local information. Global capabilities permit a global and regional laydown of stationary emitters and aid analysis of the characteristics of mobile ones. Local operators, however, may have to supply data on short-range and fleeting emitters. The optimal mix calls for a split responsibility, with global sources unfolding the map, so to speak, while local operators populate it with quick data and respond rapidly to what it shows.

Navigational Warfare

Commanders want to know where their assets are and to deny the enemy comparable information. These days, this is done by manipulating privileged access to the GPS signal, a specialized form of electronic warfare.

Because DoD owns the GPS constellation, military signals are several orders of magnitude more jam-resistant than commercial signals

(although such signals help users decrypt military signals). Military receivers (e.g., pointing to the location of GPS satellites and nulling side signals) can add yet more orders of magnitude—but receivers are available to both sides.

If tweaking one's reception suffices for defensive navigational warfare, defense is purely local (but refreshing the GPS constellation with satellites to produce harder signals helps). If tweaking is insufficient, forces may have to take more active measures, e.g., calibrating and distributing pseudo-lites to generate alternative navigational signals or detecting and neutralizing hostile jammers (some in missiles or vehicles). The latter may require sensors on the ground, the air, and space for localization.

The task of blocking enemy access to navigational data entails jamming and perhaps deception. Doing so requires knowing roughly where the enemy sits. Even with all that, success may be elusive: Maps with precisely located landmarks plus inertial navigation systems can substitute for GPS.

Thus, the passive avoidance of navigational warfare is largely a local responsibility. But finding and neutralizing enemy jammers to enhance GPS reception or proliferating jammers to degrade enemy reception requires sensors in all media and thus global information.

OTHER STRATEGIC MISSIONS

Strategic missions are those that can affect the outcome of a conflict or confrontation in important ways beyond their effects on U.S. warfighters. Chemical and biological warfare, long-range missiles, and terrorist attacks on military facilities (in peacetime) are often employed for their global psychological effect. Conversely, DoD's ability to offer allies precision battlefield information may serve U.S. interests without involving U.S. military operators directly. Border patrol in peacetime is used to characterize and counter infiltrators that range from illegal migrants to raiders and invaders. Table 2 summarizes the missions and the key parameters that influence whether supporting information is better sourced locally or globally (general intelligence aside).

Table 2

Summary of Parameters for Other Strategic Missions

	Sensors	Correlation	Purpose	Urgency	Other	Thus,
Chemical and biological warfare	Local	Yes	Global	High		Moderately local
TMD	Mostly global	No	Mostly global	Very high	Tight sensor-sensor loops	Moderately global
Force protect	Local	Some	Mostly global	Low		Entirely local
Military information assistance	Mixed	Yes	Global	Medium	Political sensitivity	Primarily global
Border patrol	Mixed	Yes	Global	High		Mixed[a]

[a]The friendlier the border, the more that local information matters.

Protection Against Chemical and Biological Attacks

Cities or military encampments may one day be protected from the consequences of chemical and biological attacks by systems that detect and broadcast indicators of dangerous compounds in the air or ground. How? Chemical and biological sensors tend to be local. Space-based sensors cannot pick up vapors, and whatever signatures they catch via, for instance, laser excitation and spectral analysis are almost always more efficiently acquired by airborne or ground-based suites. Sensor suites, if costly, may have to be globally allocated (and programmed) against threats of the highest priority, but they would have to be installed, tuned, maintained, and tested locally. Any emergencies arising from conditions that such sensors detect would be used to activate local resources (e.g., first responders) before global ones.

Yet this is not an entirely local mission. Terror is used to influence decisionmakers by holding a nation or its military at risk. Consequence management often requires getting help from off base or out of town (as is also true for floods, fires, and other weather emergencies). Some biological weapons spread diseases that can propagate beyond the immediate area (and if quarantines are needed, they are almost always imposed from without). Patterns of suspicious activity that do not, themselves, trigger responses may indicate new threats or signal the local presence of global terrorists (conversely, knowledge of local conditions is important for understanding anomalous sensor readings that, out of context, do *not* indicate attack).

Thus, the operation of a sensor suite designed to defend cities and military facilities against chemical and biological attack mixes global and local elements. Sensor maintenance is an on-site function that may require globally organized cadres; analysis must be sensitive to local knowledge of local conditions. Global reporting remains a must.

Theater Missile Defense

Defending fixed sites against theater missiles is a complex mission that requires the coordination of multiple sensors and interceptors (assuming that attacks on launchers are considered elsewhere). Sensor tasks run the gamut from launch detection (e.g., via SBIRS-High),

through track determination (e.g., via SBIRS-Low), and missile localization (for informing firing and tracking). The latter is supported by airborne radars (e.g., for boost-phase intercepts), possible UAV-based radars (same purpose), freestanding ground-based radars (e.g., the Ballistic Missile Early Warning System [BMEWS]), and guidance radars associated with interceptors. Missiles also carry radars. Finally, fast BDA is important to trigger reengagements. For the most part, TMD information comes from TMD engagement systems and not through ancillary sensors.

The greatest stress factor is being able to integrate, in real time, readings from sensors and cross-cue the sensors and interceptors of many tiers. Every element of what should be an integrated system is working on the same problem at once. Plausibly, a response may have to be choreographed with all three services and perhaps an ally (i.e., for terminal defense). Finally, if striking missiles carry chemical or biological warheads, people need to be warned immediately. Except for terminal defenses and consequence management, everything about TMD is more regional than local. Radar signals from upper-tier systems need to feed lower-tier interceptors, and sometimes a lower-tier radar can assist upper-tier interceptors and lasers.

Thus, information to support TMD (notably search rather than targeting radars) should, not surprisingly, be considered theater-level and thus regional.

Force Protection

Defending U.S. military facilities in peacetime against terrorists requires three types of information. One is intelligence on the local nature of the threat (e.g., suspicious activities) to build good physical defenses and develop standard operating procedures. Two is intelligence on specific threats so as to be warned of imminent attacks and develop immediate security procedures (e.g., who and what to scrutinize). Three is hard news of an attack in progress to employ countermeasures or mitigate consequences. The first two have global components; the last is entirely local. Base commanders are justifiably made responsible for securing their own facilities.

Is threat intelligence collection a local task? No obvious distinction exists between collecting against general threats (e.g., terrorist

recruitment) and collecting against specific threats (e.g., terrorists about to strike). Having base commanders run anything more than occasional intelligence collection of their local areas is problematic. But intelligence sharing has its usual problems: Providers like to obscure sources and methods; recipients may not believe the conclusions if they do not know how they were formed.

Thus, threat intelligence, despite its local component, has to be a global responsibility. Response systems (which make only modest use of such intelligence) are local.

Military Information Assistance

Assisting friends by providing them with defense information can bolster their defenses, not least by permitting them to target adversaries far more precisely and hence efficiently.

Such support could include background intelligence, weather reports, space-based imagery, and satellite-based communication capacity. U.S. operators offshore could also run sensors, such as long-endurance UAVs, Aegis ships, and perhaps air-dropped networked sensors (although giving allies sensors to deploy may be simpler). Other help could include maintenance software (e.g., repair manuals on CD-ROMs) and desktop (or, someday, headtop) simulator software for training. Just handling such information may require allies to have networking equipment; software; training; and what may be, in effect, an account into appropriate compartments of the COP. This assumes allies can maintain and troubleshoot the equipment they get. Otherwise, the number of U.S. contractors in country could become tantamount to a major deployment, with all the entailed sensitivities.

Central accountability and the need to create a standard synoptic picture argue for a global responsibility. So do security concerns (i.e., revealing sources and methods) that arise when others get access to U.S. information flows. This is more true if there are no in-theater forces apart from liaison personnel.

Thus, military assistance has strong global components, especially when such information streams are consolidated before shipment.

Border Patrol

This entails detecting and then countering anything that approaches a hostile border (e.g., the Korean demilitarized zone) or, conversely, checking out and dealing with what crosses a benign border. The information collection required to protect a hostile border resembles what it takes to support standoff strikes: an ability to monitor a large swath of land, coastline, and airspace; detect anomalous activity quickly; identify and classify what and who it is; and, if it is hostile or threatening, bring force to bear on it. When crossed borders carry global implications, can be scanned through global sensors, or call for the theaterwide mobilization of resources, the information requirements tend to be global.

Contraband, criminals, and illegal migrants are the more salient threats to benign borders (e.g., the Rio Grande). Sensors there are used not to support fires but to cue forces to get a close look immediately. Rarely must forces be coordinated *en masse* to counter the intrusion. Although border activity is often aimed at the interior (e.g., getting drugs or illegal migrants into the big city) and flows usually look for the weakest part of the barrier, national-level issues are rarely at stake. Global sensors are rare (border aerostats being a notable exception). Thus, the information requirements tend to be local.

The mix between "eyeballs" and sensors varies. High importance, short borders, shallow frontiers, high population density, and dense but passable terrain favor eyeballs. Coast Guard operations, by contrast, tend toward long, deep borders, low population density (e.g., fishing boats), little threat, and open and passable terrain. Their threat mix tends to favor sensors (and a few fast patrol craft).

Thus, an information system that helps guard a hostile border should be more global than local, and one that guards a benign border should be more local than global—but both would be mixed systems.

COMBAT OPERATIONS

Nine combat operations are discussed. Two are naval: fleet air defense and sea control. Four involve aircraft and other long-range strike assets: SEAD and countering air forces, striking immobile tar-

gets, striking other targets, and providing close air and artillery support. Three use ground (or littoral forces): maneuver, close-in combat, and peace operations (e.g., urban patrol). Table 3 summarizes the missions and the key parameters that influence whether supporting information is better sourced locally or globally (general intelligence aside).

Fleet Air Defense

The U.S. Navy is developing an integrated defense against cruise missile attacks that may also be applied against theater missiles and aircraft that leak through carrier air wing defenses.

The Cooperative Engagement Capability (CEC) melds readings of various radars (e.g., Aegis, Hawkeye) to build and broadcast a consolidated incoming track used to direct interceptors (i.e., Standard missiles). Plans are under way to add radars from the Army (e.g., the Patriot) and Air Force (e.g., the Airborne Warning and Control System [AWACS]) to consolidate track calculations. With the Navy years ahead of other Services in interconnecting radars, it still makes more sense for Army and Air Force radars to connect with the CEC for track construction in littoral areas rather than have the Navy net out.

Except against ballistic missiles (with their characteristic infrared plumes), today's space sensors are not used to build tracks. Whether the moving-target indicator (MTI) radars of tomorrow's Discover II constellation can pick up low-observable cruise missiles is still to be determined.

The characteristics of this mission strongly emphasize local (in Navy terms, a carrier group's coverage of several hundred kilometers) rather than global responsibility. Although the mission is insensitive to local exigencies (e.g., what the commander was trying to do at the time), the threat itself has a short to medium range and moves quickly. Communicating outside the carrier battle group gains little of use—not processing power, real-time intelligence, or higher-level guidance. With limited bandwidth coming off a ship (even with CEC) and the great time urgency, much can be lost by even trying to go outside. Thus, an information system to support fleet air defense is, with today's sensors, a local responsibility, albeit with some joint oversight to ensure compatibility between the radars of other Services and the CEC.

Table 3

Summary of Parameters for Combat Missions

	Sensors	Correlat -ion	Purpose	Urgency	Other	Thus,
Fleet air defense	Local	Yes	Regional	High	Littoral air defense needs link with Army air defense	Entirely local[a]
Sea control	Mostly global	Some	Global	Medium		Moderately global[b]
SEAD , counter-air	Mix	No	Regional	High		Mixed
Ground attack, fixed	Mostly global	No	Global	Low	Local BDA for restrike	Moderately global
Ground attack, mobile	Mostly local	Yes	Regional	High	Sensor integration is key	Moderately local
Close support	Local	No	Local	Very high		Entirely local
Maneuver	Mostly local	Some	Local	Very high		Moderately local
Close combat	Local	No	Local	Very high		Entirely local
Peace operations	Mixed	Yes	Local	High		Moderately local

[a]Littoral operations that require tight coordination with Army and U.S. Air Force air defense units may require moving responsibility up.

[b]Distinctions among ships (e.g., for blockades and small craft) may require local information.

Sea Control

Keeping hostile ships and submarines out of designated waters has historically entailed defeating the enemy's fleet once at sea. Today, there is little reason a ship cannot also be put in peril in port. Finding ships is relatively straightforward. Submarines are harder to detect, harder to engage (particularly from far away), and often bunkered. Blockade enforcement is complicated by the need to identify commercial shippers of proscribed goods and dissuade them from crossing a line.

The information that is needed to find clearly military ships is increasingly shifting from local to global. Ships are hard to hide (and stealth is a relative term when describing naval vessels). A combination of sea-scanning satellites (with SAR/MTI, electro-optical, and ELINT sensors), and UAVs (with similar sensors) positioned over likely transit areas makes discovery only a matter of (not much) time. Once seen, ships can be shot at from long distances (e.g., cruise missiles). Until the population of satellites and UAVs is sufficiently dense, those looking for ships will be forced to comb through a heterogeneous mass of sensor readings, some held by third parties (e.g., commercial satellites, shore-based Webcams, and fishermen with cell phones), thus requiring global correlation.

Finding a nonobvious craft on the seas is but one part of a cue-filter-pinpoint process. The craft may merit a closer look by local UAVs; its signature may have to be correlated against an intelligence database; and it may have to be boarded or at least drawn close to. Ships in a position to do this may need external help in analyzing what they find (e.g., much as the police call in license plates) or receiving command guidance (e.g., the Cuban Missile Crisis), but, otherwise, they must often make decisions on the spot with subsequent reporting. Maintaining the contact database, however, is important.

Searching for submarines requires global sensors, such as SOSUS arrays (and perhaps an analysis of ocean surface effects collected by spacecraft), and local sensors (e.g., ship-based sonar and sonobuoys), all complemented by occasional surface sightings. Again, building and maintaining a global contact file (including noises that sound like contacts but are really distant surface vessels or marine life) helps. The cue-filter-pinpoint process is at work here, but, bar-

ring the development of persistent sonobuoys, the bulk of the information and almost all of the engagements are local.

Thus, an information system for sea control is likely to have both global and local elements. Ship and submarine detection is becoming increasingly global. Overlaid on this, local means are required for surface ship discrimination, submarine localization, and battle management. Information support for sea control is a split responsibility.

SEAD and Counter-Air

Suppression entails (1) finding and disabling opposing radar-missile sites; failing that, (2) inhibiting adversaries from turning on their radars; or, failing that, (3) confounding their engagement systems through electronic warfare and other antisensor techniques. Counter-air operations entail destroying opposing aircraft and support facilities (e.g., runways, control towers, and fuel depots), as well as inhibiting the survivors from offering effective opposition.

The knowledge required to do SEAD contains both global and local elements. To some extent, ELINT satellites can acquire radar signatures and can, in theory, transmit their rough coordinates in real time. In the future, networks of ELINT UAVs should offer greater positional accuracy, and perhaps faster reportage. Both tend to be global or at least regional information systems. Suppressing man-portable antiaircraft defenses (e.g., Stingers) may require either ground control (unlikely if flying deep), a dense sensor network, or some ability to detect the infrared signature of the missile and return fire quickly.

The information required for air superiority includes surveillance data to pick out aircraft from the clutter; early warning data; and finally, aircraft-radar targeting data. Such data are, at most, lightly fused because they have very separate time domains (e.g., persistent versus evanescent data) and space domains (e.g., sensors used to read the ground differ from those used to track aircraft in flight).

For both the SEAD and air superiority missions, after-action reports to fill an intelligence database are very helpful.

Thus, information for both missions is layered. A global database fed from multiple sensors and occasionally fused (notably by correlating

ELINT and ground sensor data) forms a background that informs strike operations. When fed to pilots, the global database becomes the mental template on which local information (the last category) is applied and exploited, literally, within seconds or fractions thereof.

Standoff Attacks and BDA on Fixed Ground Targets

Attacking fixed ground targets is best done from standoff range (unless they are scattered and merit great tonnage). The information required is knowing what the targets are and where they sit.

Generally, a target list is built from persistent intelligence aided by space-based sensors (electro-optical, SAR/MTI, hyperspectral) and their air-breathing counterparts supplemented by ground observation from soldiers, spies, and civilians plus everyday data. Combat itself creates information that may reveal key facilities (e.g., because soldiers are observed leaving from it). All these data would be combed and crunched. Sensor data (because of their embedded geospatial references) can usually be applied immediately to maps (even if the identity or purpose of some fixed facilities is undetermined). Further analysis helps rank potential targets (e.g., this facility is a critical node, but that one is standby) and assess their interrelationship (e.g., hit these five targets simultaneously; otherwise, the adversary will just keeping shifting assets from one to the other). Ultimately, these data can be logged to a master geospatially cross-referenced database.

For BDA, unless a target's destruction is obvious (a problem if nonlethal munitions are used), evidence of activity is required to determine whether the target is still functioning. Electronic emissions, movement, heat, smoke, or vapors are all indicators of activity. The first three may be captured from afar, as well as from up close. BDA can also come from pilots. Some next-generation weapons may carry trailing sensors that provide instant BDA. Rapid acquisition is important if the same strike package is to turn around for another strike.

Notwithstanding targets of opportunity (e.g., one whose characteristics are not clear until it does something or until someone gets right next to it), the decision to destroy fixed ground targets tends to be global, and so is the choice of which standoff weapons to use (it can be made by the CINC or by assigning sectors to units).

Thus, the logic of a master database, the importance of global sensors, the role of reach-back analysis, and the fact that fixed targets may be hit by many standoff weapons all suggest that global information systems support striking standoff targets. But BDA for immediate restrike tends to need local information.

Standoff Attacks on Other Ground Targets

Other targets include those that (1) have distinct signatures but are hidden or bunkered until moved or fired, (2) are visible but hard to identify as hostile (or worthwhile) until some event occurs, and (3) are suddenly encountered at close range. Mobile targets may not stay open very long if they leave sensor range, go under cover, or are lost within clutter (raising the possibility of collateral damage).

Hard-to-find targets (e.g., Scuds) are often recognized and localized by scanning large areas, analyzing them, and converting findings into aim-point tracks for operators who are standing (or flying) by—a global process that requires global information.

To strike ambiguous or sudden targets, it often helps to have command knowledge (e.g., "now look for this") and combatant knowledge (e.g., "now chase that"). The faster the target can flee after being out in the open, the closer the shooter must be. Sensors used against fleeting targets should be sensitive to their moving (detectable by MTI radars, acoustic sensors, or chemical sensors keyed to engine combustion) or shooting (detectable by counter-battery radar or by infrared, acoustic, or chemical sensors). Acoustic, chemical, and some counter-battery radar and infrared sensors tend to have short ranges and are thus local, but fields of networked sensors, particularly if remotely placed, are more global. Some MTI and infrared sensors have long ranges and are thus global or at least regional. Operators (who stumble onto foes or who gather data through contact that cause foes to be reassessed) are local.

Operators trying to engage such targets on their own would have to fuse what they see (data coming in from their eyes) with what they hear (data coming in from their ears, notably command decisions), layering it atop data already in their heads (or on screen—the common tactical picture as determined from intelligence reports and active sensors).

Thus, here too, the information system required to catch such targets mixes local and global elements—more likely, local elements layered atop information from global elements. The swing element is who lays down, manages, and harvests data from tomorrow's networks of short-range sensors and whether they are hand deployed (and thus locally operated) or remotely placed (e.g., by aircraft but possibly rockets and artillery) and thus monitored.

Close Fire Support

Air and artillery support is akin to hitting a fleeting target except that (1) avoiding hitting one's own forces is a major constraint (operations to "soften up" an area are similar but carry less risk of friendly fire) and (2) precision is unnecessary if the density of targets in the strike area is high. Sensors may not pick up distinctions between friend and foe very well, and their data can often not be analyzed fast enough anyway.

When friendly forces cannot be evacuated, it might be possible to avoid hitting them by aiming away from where they are or, one day, by equipping all rounds with a precision capability that *avoids* programmed aim points associated with friendly forces (reporting GPS coordinates) or sensitive collateral targets (e.g., medical facilities).

Minimizing risks to the shooters (e.g., hostile air defenses, counter-battery assets) will require both intelligence on hostile forces and (in the case of close air support) air monitors (local).

Thus, the close fire support, being a local matter, is largely supported by local information.

Maneuver

Forces in motion prefer not being detected (or at least not until they can defend themselves). Failing that, quick news that they are discovered helps them react in time. This holds for ground, air-mobile, and littoral maneuver.

Much of the information needed for maneuver is local: scouting for adversaries or not-so-innocent spectators, querying not-so-hostile spectators to assess what they know, and monitoring one's own signature to control it. Successful maneuver also involves persistent

and current intelligence of the land. Sensors may be useful in the seemingly contradictory tasks of monitoring signature control and in locating one's own forces (when radio silence is a must).

Knowing what the enemy does not know of one's movements is hard. Some clues may come from knowing where they and their sensors are *not*. But not finding does not prove nothing is there to find. Rather than attacking all adversaries whenever spotted, one should be able to infer their knowledge from their movements (e.g., going into attack formation suggests they spotted something). Intercepting communications and computer data might help.

Thus, the information to support maneuver is quintessentially local, but any global information on what the adversary knows (e.g., based on intercepting what they report back) would help.

Close Combat

Close combat (ground and littoral) exists to flush out and destroy enemy forces otherwise inaccessible through long-range strike, as well as occupying contested terrain. Inaccessibility comes from the inability to find and identify targets precisely or to strike targets once found—at least without unacceptable collateral damage that may result from the intermix of friendly, hostile, and neutral elements.

Close combat can be quick. Foes are maneuvering unpredictably relative to the killing radius of one's weapons (which are measured in centimeters to meters) and obstacles (e.g., buildings). They often shoot back and thus must be suppressed. A great deal of information is being collected by one's own warfighters. Compared to other missions, warfighter communications (and GPS) are likely to be more important and sensors less so. Nevertheless, acoustic, thermal, and wall-penetrating sensors that can localize gunfire and gunfighters would help and are usually local.

Some overhead sensors may be able to track open movements (e.g., an enemy squad running from cover to cover). They would have to operate right over the battlefield for good lines of sight, probably close to the ground to make good distinctions. Fighting over terrain wired for sight and sound also helps but can rarely be expected and is inconceivable in some cases (e.g., forced entry). Generally speaking, such sensors need to be under local control because they must

respond quickly to the insights and strategies of the commander on the scene. By contrast, synoptic sensors may do more harm than good if warfighters cannot easily locate themselves and their foes in an image taken from an external perspective (aural data representation, if possible, may work far better than visual displays).

Connectivity outside the battlefield may occasionally be helpful if warfighters want to tap cohorts with useful tips on how to operate in similar situations or to receive analysis on certain sensor readings (e.g., the spectral analysis of an unknown scent). When calm returns, warfighters may have material to contribute to a systematic lessons-learned knowledge base.

Finally, modern militaries would prefer to avoid close combat (even as their foes would prefer it, for the same reasons) and often find themselves engaged because of knowledge *failures*.

Thus, the conduct of close combat clearly requires local information, although access to global services helps.

Peace Operations

The aim of peace operations is to limit violence in environments potentially characterized by factions, gang warfare, street disturbances, and the widespread (but not necessarily total) distrust of authority.

In many ways, peace operations resemble force protection. Both rely on a combination of good neighborhood intelligence, rapid appreciation of threats, and quick detection of disturbances. But force protection takes place within the perimeter of control; patrol operations take place beyond it.

Do sensors matter? External sensor coverage detected the illicit possession of heavy weapons by all sides in Bosnia. But sensors alone cannot inform decisions (e.g., tanks whose owners are undetermined are not automatically destroyed). Their data are more likely to prompt commanders to move forces into an area so that they can make distinctions (e.g., are the technicals armed? Who mans them? Why?). Sensor data can also be used to gather evidence on crimes for law enforcement.

Global sensors tend to be adjuncts. The important information sources are intelligence and other warfighters (including allies) supplemented with helpful hints from residents and perhaps local sensors (e.g., street-post cameras). Taps to external expertise (e.g., to assay what is burning out there) may help.

Thus, peace operations require a local information system that can use global input depending on the time criticality of response (faster means more local) and the advantages of humans versus sensors (density favors people).

COMBAT SUPPORT

The three missions analyzed are lift (and thus traffic control), material management, and field health services. Table 4 summarizes the missions and the key parameters that influence whether supporting information is better sourced locally or globally (general intelligence aside).

Lift and Traffic Control

Managing transport vehicles of all Services (and sometimes those of allies and commercial enterprises) is key to material delivery. Few, if any, sensors are required to support individual vehicle movements. Knowing where one is and perhaps where neighboring vehicles are should suffice. Ancillary information on weather, traffic conditions, and hazards profits from sensor inputs.

Local information is needed for maneuver in tight locations (e.g., airports, air traffic corridors, seaports, narrow passages, rail yards, and potentially congested highways). Data on the availability, location, and loading of transport vehicles ought to be reported globally to optimize scheduling (the expected completion of which informs deployment plans) and permit traffic controllers to act ahead (e.g., opening up a runway, hustling ships out to sea).

Global MTI (e.g., Discoverer II but also forthcoming UAVs) could let global sensors substitute for local ones in traffic management. Yet, the trend (at least in U.S. air traffic control) is toward local self-optimization; after spending billions on the new air traffic control

Table 4

Summary of Parameters for Support Missions

	Sensors	Correlation	Purpose	Urgency	Other	Thus,
Lift	Mostly local	No	Regional	Low	Asset mobilization	Moderately local
Logistics	Local	Yes	Local	Low	Asset mobilization	Moderately global[a]
Medical	Local	Some	Local	Very high		Entirely local

[a]Locally collected, but globally accessible.

system, the Federal Aviation Administration is moving toward "free flight," under which aircraft declare their intended air space, use GPS to stay within it, and deconflict competing claims directly with others. Similarly, the allocation of congested transport nodes may be negotiated among users, each of which is given a pseudo-budget with which to buy or sell access—but such methods are untested and may be inconsistent with the military culture of command and control.

Thus, global knowledge of vehicle location and availability is a good thing, and global knowledge of traffic conditions lets others forecast the availability of vehicles and scarce transportation infrastructures. But real-time traffic control (where factors are measured in minutes and seconds, not hours and days) is generally a local responsibility and may devolve to an individual vehicle responsibility.

Material Management

The purpose of logistics is to deliver, return (in the case of repairables), and manage both the flow of material and information on its delivery times.

With rare exceptions (depot-level repairable, facilities management), logistics is a global system because it reaches back into U.S. warehouses and manufacturers. Information on material is used both to manage the logistics system and to feed operational planning; it too must be global.

Traditionally, each Service has performed its own logistics, thanks to the belief that the demands of each overlap little with the others and the suspicion that no one Service in charge would be even-handed or responsive to its counterparts (DLA, despite being managed by military officers, is not entrusted with much more than commodities).

Yet, the requirement that the various logistics information systems be interoperable is difficult to ignore—and not only because networking has lowered the cost of doing so. Infrastructure consolidation will raise the number of joint logistics facilities, while the use of commercial off-the-shelf technologies (especially in information technology) and products from the growing roster of joint programs (e.g., the Joint Tactical Information Distribution System) increases

the commonality between what each Service is using. The push for jointness has hiked the urgency of each Service's having visibility into the readiness of its counterparts. The cost of equipping, maintaining, and training users on logistics workstations can be trimmed if each Service uses common or at least mutually interoperable software packages and data formats (e.g., the Global Combat Support System).

Thus, even if four (three Services and DLA) separate logistics systems remain, four stovepipe logistics *information* systems make no sense. One large system may not be necessary, but each system should be mutually accessible. This, in turn, means that each should use compatible data structures and software packages (making the responsibility for *engineering* logistics information systems potentially global).

Field Medical Triage and Care

Medics must rapidly evaluate the wounded, evacuating some and treating the rest. Traditionally, medics worked entirely with local knowledge. But global information is increasingly being called on: patient medical records, current data on regional medical facilities (e.g., their loading), and telemedicine (via query, visual inspection, or sensor analysis). At the same time, miniaturization can bring more of the hospital forward. Medical records are being put onto smart cards (often worn like dog tags). Soon, palmtop devices will be able to store a battalion's medical records, overnight status reports of all regional field hospitals, programs for medical analysis, and expert systems (e.g., if the condition is this, do that). Forthcoming laboratories-on-a-chip can assay blood. Future medical devices may use ultrasound or infrared measurements to evaluate injuries and internal bleeding. In some cases, this will substitute for a remote expertise; at least, such devices provide all the more data for outside experts to chew on. Thus, field medicine is inherently local, but connectivity to global expertise (entailing both experts and knowledge bases) is likely to remain important.

Traditionally, information provided to warfighters only gave them broad situational awareness. Today, information from sensors and databases can help warfighters target past what they can see. This has prompted the Department of Defense (DoD) to build a military analog to the Internet, to be a font of warfighting information (and system services). But how should responsibility for providing information and services be shared between global external sources and organic local sources? Both will be necessary, and sensor characteristics matter. But sometimes the need for integrated battlespace pictures (e.g., the Recognized Air Picture) pushes responsibility higher. Thus, tools are needed to let commanders use whatever information from whatever sources fits their needs at a given time. A strong bias toward interoperability would foster universal access to information. Liberal distribution of unit-level sensors and connectivity should help warfighters develop and share operational information. And better technology is needed to marry local and global information sources more easily. Finally, some entity within DoD should review current information services and lay out a road map for filling in the blanks.

ISBN 0-8330-2888-X

9 780833 028884 51400

MR-1247-AF